

7. Indukce a rekurze

Na matematickou indukci jsme již v této knize několikrát narazili v důkazech. Spoléhalí jsme na to, že se čtenář s ní již setkal. Obvykle je to ale setkání s formalizovaným postupem pro dokazování rovností, který představuje jen nejjednodušší podobu indukce a není úplně reprezentativní. V této kapitole tuto jednoduchou podobu postavíme na pevný základ a posléze rozšíříme na mocný nástroj.

7a. Matematická indukce

Matematická indukce ve skutečnosti není jeden formální postup, ale základní myšlenka, která má podle potřeby mnoho podob. Z pokročilého pohledu je tak indukce jedna, nicméně pro začátečníky bývá užitečné rozlišit několik populárních přístupů. V této sekci začneme tou nejjednodušší podobou, kterou čtenář nejspíše už potkal.

Představme si, že zkoumáme určitý jev, který vede na různé situace. Všimli jsme si něčeho, co by mohlo platit pro všechny situace, a chceme to potvrdit důkazem. Abychom mohli použít indukci, musí se povést dvě věci. Za prvé, situace dokážeme očíslovat pomocí celých čísel počínaje nějakým n_0 . Pokud například zkoumáme autobusy MHD ve městě, tak můžeme sledovat jejich pozice v hodinu n . Nebo můžeme chtít něco o nich potvrdit v závislosti na tom, že je jich zrovna n ve službě. Asi se najdou i další možnosti.

Druhou podmínkou je, že se nám podaří najít vztah mezi situací s indexem n a tou s indexem $n + 1$. Intuitivně, snažíme se určit, co se stane v bezprostřední budoucnosti, na základě přítomnosti. Pokud se to povede, pak má smysl zkusit použít důkaz indukci.



7a.1. Slabý princip matematické indukce.

Nechť $n_0 \in \mathbb{Z}$, nechť $V(n)$ je vlastnost celých čísel, která má smysl pro $n \geq n_0$.

Předpokládejme, že:

(0) platí $V(n_0)$.

(1) Pro každé $n \in \mathbb{Z}$, $n \geq n_0$ je pravdivá následující implikace:

Jestliže platí $V(n)$, pak platí také $V(n + 1)$.

Potom $V(n)$ platí pro všechna $n \in \mathbb{Z}$, $n \geq n_0$.

Weak principle of mathematical induction. Let $n_0 \in \mathbb{Z}$. Let $V(n)$ be a property of integers that makes sense for $n \geq n_0$. Assume that the following conditions are satisfied:

(0) $V(n_0)$ is true.

(1) For every integer $n \geq n_0$ the following implication is valid: If $V(n)$ is true, then $V(n + 1)$ is true.

Then $V(n)$ is true for all $n \geq n_0$.

The part (0) is called the base step, (1) is called the induction step.

Indukce bývá často přirovnávána k lezení po nekonečném žebříku. Když ukážeme, že platí tzv. **základní krok** (0), tak víme, že umíme vylézt na jeho první příčku. Tzv. **indukční krok** (1) zase ukáže, že když už někde na žebříku jsme, tak umíme vylézt o příčku výš. Podstatný je ten obecný kvantifikátor v (1), indukční krok je splněn pro libovolné místo na žebříku. Intuice říká, že pak už se dostaneme na žebříku všude.

! **Příklad 7a.a:** Indukce byla na intuitivní úrovni používána již indickými a arabskými matematiky kolem 10. století. Poprvé byla přesně formulována Pascalem v roce 1665, ale intuitivní použití v Evropě sahá do 16. století. Údajně první byl F. Maurolico, který tak dokázal, že součet prvních n lichých čísel (myšleno kladných) je n^2 . Předvedeme na této úloze správný postup a okomentujeme jej.

Nejprve si rozmyslíme, že prvních n kladných lichých čísel se dá zapsat následovně:

$$1 + 3 + \cdots + (2n - 1) = \sum_{k=1}^n (2k - 1).$$

Například pro $n = 3$ vzorec nalevo („třítečková verze“) dá $1 + 3 + 5$, tedy první tři lichá čísla. Výhodou tohoto vzorce je intuitivní zjevnost. Nevýhodou je, že není zcela matematicky korektní (co jsou tři tečky? co když $n = 1$?). Budeme jej tedy brát jako populární zkratku pro přesný výraz napravo („sumační verze“). Obě jsou v důkazech indukci populární, třítečková verze bývá delší na psaní, ale názornější.

Nyní dokážeme indukci, že součet je n^2 . Abychom ukázali, jak princip aplikujeme, budeme se formálně odvolávat na $V(n)$. Někdy se tak důkazy indukci zapisují, ale pro zkušené indukčníky je jednodušší pracovat bez tohoto formalismu, což uvidíme v následných důkazech.

• *Zformulujeme přesně tvrzení a oznámíme, jak jej dokážeme.*

Pro $n \in \mathbb{N}$ je $V(n)$ tvrzení, že $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

Dokážeme to pomocí matematické indukce.

- *Dokážeme základní krok pro nejmenší uvažované číslo.*

(0) Necht $n = 1$. Vlastnost $V(1)$ zní $1 = 1^2$, což je pravda.

- *Dokážeme indukční krok. Vezmeme libovolné $n \in \mathbb{N}$ (obecné, ne nějaké konkrétní) a dokážeme, že pro něj platí implikace $V(n) \implies V(n+1)$. To se typicky dělá přímým důkazem, takže předpokládáme, že pro naše zvolené n platí $V(n)$, tomu se říká „indukční předpoklad“. Pomocí něj pak dokážeme platnost $V(n+1)$. Na to je třeba najít nějakou souvislost mezi tím, co dokazujeme pro n , a obdobným tvrzením pro $n+1$. Někteří autoři tomu říkají dekompozice.*

Obvykle je dobré začít od cíle a hledat v něm předpoklad. My chceme dokázat platnost $V(n+1)$, tedy rovnost získanou tak, že všechny výskyty n v dokazované rovnosti nahradíme výrazem $n+1$. Dostaneme $1 + 3 + 5 + \dots + (2(n+1) - 1) = (n+1)^2$ neboli $1 + 3 + 5 + \dots + (2n+1) = (n+1)^2$. Potřebujeme najít souvislost s rovností $V(n)$. Zde je klíčové si všimnout, že když jsme v součtu nalevo přešli od n k $n+1$, tak již existující čísla zůstala a přibýlo jedno navíc. Konkrétní příklad často napoví:

$$n = 5 : 1 + 3 + 5 + 7 + 9$$

$$n = 6 : 1 + 3 + 5 + 7 + 9 + 11$$

Obecně:

$$n : 1 + 3 + 5 + \dots + (2n - 1),$$

$$n + 1 : 1 + 3 + 5 + \dots + (2n - 1) + (2n + 1).$$

Vidíme tedy, čím se liší levé strany ve $V(n)$ a $V(n+1)$, což nám umožní mezi nimi přejít v důkazu implikace.

- (1) Necht $n \in \mathbb{N}$ je libovolné. Předpokládejme, že platí $V(n)$: $1 + 3 + 5 + \dots + (2n - 1) = n^2$. Když k oběma stranám připočteme $2n + 1$, dostaneme

$$\begin{aligned} 1 + 3 + 5 + \dots + (2n - 1) &= n^2 & / & + (2n + 1) \\ 1 + 3 + 5 + \dots + (2n - 1) + (2n + 1) &= n^2 + (2n + 1) \\ 1 + 3 + 5 + \dots + (2n + 1) &= n^2 + 2n + 1 \\ 1 + 3 + 5 + \dots + (2n + 1) &= (n + 1)^2 & \text{potvrzeno } V(n + 1). \end{aligned}$$

- *Uděláme závěr.*

Důkaz je hotov.

□

Když z toho důkazu výše vynecháme vysvětlující části psané kurzívou, dostaneme důkaz tak, jak se běžně zapisuje. Všimněte si, jak u dalších důkazů zachováváme tuto strukturu.

△

S 7a.2 Poznámka: Tento důkaz je správný, nicméně pro důkaz indukčního kroku doporučíme a budeme používat jiný přístup. Použité přímé odvození závěru je přirozené a korektní, ale nedostatečně flexibilní a navíc zbytečně dlouhé. V poznámce 1a.18 jsme doporučili alternativu pro případ implikace, u které má závěr podobu cesty, což je také případ rovnosti. V našem případě tedy doporučovaná struktura vypadá tak, že po volbě n , se kterým pracujeme, nejprve stanovíme indukční předpoklad, tradičně značený (IP), ale pak z něj nevyjdeme. Místo toho budeme rovnost pro případ $n+1$ dokazovat tak, že začneme na jedné její straně a postupnými kroky dojdeme na druhou. Někde cestou použijeme indukční předpoklad. Bývá dobrým nápadem ještě předtím čitatele varovat, co budeme dělat.

Je dobré začít naši cestu tou stranou, u které vidíme dekompozici neboli souvislost případu $n+1$ s případem n . Obvykle je to ta komplikovanější či delší strana, zejména to platí pro součty a násobky (mocniny, faktoriál).

Cestovací přístup také nabízí efektivní zápis pro ověření rovnosti v kroku (0).

△

Doporučený postup a zápis teď předvedeme návratem k prvnímu příkladu. Ukážeme zde zápis důkazu, kdy nebudeme pracovat se značením $V(n)$, ale přímo s dokazovanými rovnostmi. Použijeme sumační značení, u kterého máme pohodlný způsob oddělení přidaného členu pro verzi $n+1$.

- ! **Příklad 7a.b** (návrat k 7a.a): Dokážeme indukcí, že pro $n \in \mathbb{N}$ platí

$$\sum_{k=1}^n (2k - 1) = n^2.$$

$$(0) \ n = 1: \sum_{k=1}^1 (2k - 1) = 2 \cdot 1 - 1 = 1 = \underline{1^2}. \text{ Ověřeno.}$$

(1) Dáno $n \geq 1$. Předpokládá: $\sum_{k=1}^n (2k-1) = n^2$. (IP)

Dokážeme, že pak platí $\sum_{k=1}^{n+1} (2k-1) = (n+1)^2$.

$$\begin{aligned} \sum_{k=1}^{n+1} (2k-1) &= \sum_{k=1}^n (2k-1) + (2(n+1)-1) = \sum_{k=1}^n (2k-1) + (2n+1) \\ &\stackrel{\text{IP}}{=} n^2 + (2n+1) = n^2 + 2n + 1 = \underline{(n+1)^2}. \end{aligned}$$

Ověřeno.

□

Všimněte si, jak jsme indikovali využití indukčního předpokladu. Pomáhá to čtenáři, ale také nám to při psaní důkazu připomene, že máme ověřit, že jsme indukční předpoklad použili správně. To bude důležité zejména u složitějších forem indukce, viz poznámka 7b.5.

△

Technická poznámka. Krok 1 jsme zahájili volbou n , která je vymezena nerovností. Někdo by mohl namítnout, že to není správně, protože to připouští třeba i $n = \pi$. Formálně vzato by bylo lepší napsat „Dáno $n \in \mathbb{Z}$, $n \geq 1$ “ a občas se to dělá, ale obvykle ne.

Úmluva.

Když v souvislosti s indukcí napíšeme nerovnost $n \geq n_0$ s nějakým $n_0 \in \mathbb{Z}$, tak se uvažují jen $n \in \mathbb{Z}$.

Výjimky je pak třeba specifikovat.

S Poznámka: V příkladě 7a.b jsme cestu začali od levé strany, ale šlo by to i naopak. Pak bychom museli hledat návaznost mezi $(n+1)^2$ a n^2 . Zde je pro začátečníka užitečné se zamyslet nad typickými druhy chování.

U součtů přechod $n \mapsto (n+1)$ znamená, že ke stávající sumě přibude člen. V příkladě nám konkrétní případy pomohly odhalit vztah

$$\sum_{k=1}^{n+1} (2k-1) = \sum_{k=1}^n (2k-1) + (2(n+1)-1),$$

v sumačním značení je tedy snadné vidět, jak tento nový člen vypadá. Obecně platí (viz sekce 7a.7)

$$\sum_{k=n_0}^{n+1} a_k = \sum_{k=n_0}^n a_k + a_{n+1}.$$

Podobně přímočaré jsou mocniny: $a^{n+1} = a^n \cdot a$, což výmluvně napoví dlouhý zápis:

$$a^{n+1} = \underbrace{a \cdot a \cdots a \cdot a}_{n+1} = \underbrace{a \cdot a \cdots a}_n \cdot a.$$

Další takto příjemný výraz je faktoriál, který potkáme níže.

Pocitově odlišné jsou algebrické výrazy, které se přechodem $n \mapsto (n+1)$ spíše proměňují než rozšiřují o nový člen, což je třeba případ toho n^2 z dokazované rovnosti. Ale i tam potřebujeme najít návaznost na „případ n “, tedy i tam je třeba ukázat, že původní výraz se zachová a něco k němu nějakým způsobem přibude:

$$(n+1)^2 = n^2 + 2n + 1 = n^2 + (2n+1).$$

Náš důkaz tedy v kroku (1) mohl vypadat takto:

$$\underline{(n+1)^2} = n^2 + 2n + 1 = n^2 + (2n+1)$$

$$\stackrel{\text{IP}}{=} \sum_{k=1}^n (2k-1) + (2n+1) = \sum_{k=1}^n (2k-1) + (2(n+1)-1) = \underline{\sum_{k=1}^{n+1} (2k-1)}.$$

△

! Jak vlastně indukce dokazuje platnost našeho tvrzení? Díky základnímu kroku víme, že platí pro $n = 1$. Nyní aplikujeme indukční krok s volbou $n = 1$, tedy máme dokázanou implikaci $V(1) \implies V(2)$. Protože už víme, že $V(1)$ platí, tak podle této implikace musí platit i $V(2)$. Nyní aplikujeme dokázanou implikaci pro $n = 2$. Platí $V(2) \implies V(3)$ a zjistili jsme, že $V(2)$ platí, proto musí platit i $V(3)$. Pak aplikujeme implikaci s $n = 3$ atd. Je snadné si představit, že takto se pravdivost vzorce postupně rozšíří na všechna přirozená čísla.

Spíše než žebřík se zde hodí představa padajících očíslovaných kostek domina postavených na výšku za sebe. Čtenář doufejme viděl podobné sestavy, kdy po dlouhých hodinách pečlivého stavění autoři shodí první kostku domina a pak se rozjede proces, který mnohdy trvá celé minuty a krouží po rozlehlé ploše. Tato představa pro nás bude velmi užitečná. Indukční krok (1) zaručuje, že kostky jsou správně rozestaveny, a krok (0) říká, že jsme shodili tu první.

Indukce je na střední škole často představována jako jakýsi formální postup o několika krocích, který je třeba dodržovat (občas dokonce chybný). Pro správné použití je důležité dobře rozumět tomu, co se v takovém důkaze vlastně děje.

M 7a.3 Poznámka: Základní a indukční krok představují nezávislé části, které se navíc podstatně liší. Zatímco základní krok dokazuje faktickou platnost V pro jisté číslo, v indukčním kroku se o platnosti V pro nějaká čísla nic nedozvíme. Sice se v důkazech může objevit konstatování „ $V(n+1)$ platí,“ ale je to tvrzení podmíněné platností $V(n)$, nikoliv samostatný poznatek. V kroku (1) tedy zkoumáme souvislost mezi případy n a $n+1$, která ovšem může existovat i pro V , které vůbec neplatí. Víme totiž, že implikace s nesplněným předpokladem je automaticky pravdivá.

Například přičtením jedničky k rovnosti $n = n + 13$ dostaneme $n + 1 = (n + 1) + 13$. Tím jsme pro tuto rovnost korektně dokázali platnost implikace $V(n) \implies V(n+1)$ pro všechna celá čísla, ovšem tato rovnost nikdy neplatí. Viz také cvičení 7a.11.

Zvládnutý indukční krok sám o sobě nám tedy pravdivost V nedá a odpovídá tomu, že jsme správně rozestavili kostky domina. Tím je u domina nutno začít a stojí za zmínku, že také důkazy indukce je často vhodné začít od analýzy kroku (1), protože v něm je skryta podstata toho, co dokazujeme. Je důležité si všimnout, že správnost rozestavení ověřujeme nezávisle po dvojicích, nikoliv najednou pro všechny kostky. Vezmeme kostku s číslem n a podíváme se, zda je ta další ve správné vzdálenosti, aby ji předchůdkyně svým pádem dokázala shodit. Tak postupně projdeme celou dráhu.

Obdobně když dokazujeme implikaci $V(n) \implies V(n+1)$, tak to činíme pro jedno konkrétní (i když neznámé) n , které jsme zvolili libovolně, abychom důkazem pokryli všechna potřebná čísla, ale pracujeme jen s tím jedním zvoleným. To je zejména pravda o indukčním předpokladu. Ten se vyjadřuje pouze o platnosti $V(n)$ pro zvolené číslo, o jiných n nic neříká. To je klíčové pro správné pochopení a použití indukce.

Pro ilustraci se podívejme na následující důkaz, že pro všechna $n \in \mathbb{N}$ platí $n = 1$.

(0) $n = 1$: $1 = 1$ platí.

(0) Dáno $n \in \mathbb{N}$, IP: $n = 1$. Příklad $n + 1$: Napíšeme $n + 1 = 2n - (n - 1)$. Podle IP je $n = 1$ a $n - 1 = 1$, proto

$$n + 1 = 2n - (n - 1) \stackrel{\text{IP}}{=} 2 \cdot 1 - 1 = 1.$$

□

Kde je chyba? Čtenář by si měl rozmyslet, že struktura důkazu je správně, rovněž v algebře není problém. Chyba nastala při aplikaci indukčního předpokladu. Čísla n a $n - 1$ jsme nahradili jedničkou, ale IP se dělá pro jedno konkrétní číslo zvané n , zatímco $n - 1$ je úplně jiné číslo, o kterém nevíme nic! Viz také cvičení 7a.10. Klíčové to bude v následující sekci.

Je tedy důležité napsat krok (1) tak, aby z textu bylo zřejmé, že opravdu IP pracuje jen s jedním konkrétním číslem, nikoliv všemi n . Stejně tak si toho musí být vědom autor důkazu, aby neudělal podobnou chybu. Dobře napsaný indukční krok dokáže platnost nekonečně mnoha implikací

$$V(n_0) \implies V(n_0 + 1), V(n_0 + 1) \implies V(n_0 + 2), V(n_0 + 2) \implies V(n_0 + 3), \dots$$

Když máme správně rozestavena domina, je třeba to první shodit. O to se stará základní krok indukce. Ten je třeba s indukčním krokem správně zkoordinovat. Když domina správně nastavíme od kostky s číslem 6 a shodíme kostku 3, pak vůbec nemáme zaručeno, že vše správně proběhne, což odpovídá tomu, že nevznikne správný důkaz. Opačný případ tak špatně nedopadne: Pokud nastavíme kostky domina od té s číslem 3 dál a shodíme kostku číslo 7, tak se padání rozjede a všechny kostky počínaje sedmou spadnou. Obdobně nekoordinovaný důkaz by byl vlastně platný, ale jeho autor by dělal práci navíc (kontroloval nepoužité kostky), což by ukazovalo na problém s chápáním indukce.

U slabé indukce je samozřejmě zcela jasné, jak základní a indukční kroky navázat, stejné číslo n_0 musíme vidět v kroku (0) $n = n_0$ a také v hlavičce kroku (1) $n \geq n_0$. Ovšem u pokročilejších verzí indukce, které brzy potkáme, se hodnoty v hlavičce (0) a (1) shodovat nemusejí a je třeba se zamyslet. Pokud si nejsme jisti, zda máme indukci správně sestavenou, tak zkusíme pomocí toho, co jsme dokázali, přesvědčit čtenáře či sebe o fungování dominové kaskády, jak jsme to udělali s konkrétními čísly před tímto důkazem.

Ovšem aby mohl čtenář (a také autor důkazu) ověřit, že kroky správně navazují, je potřeba u indukčního kroku napsat, pro jaká n se dělá. Jinak vznikne nezkontrolovatelný a tedy nefunkční důkaz. Pro výstrahu dokážeme, že pro všechna $n \in \mathbb{N}_0$ platí $n \cdot e^n = 0$.

(0) $n = 0$: $0 \cdot e^0 = 0 \cdot 1 = 0$ platí.

(1) Předpokládejme, že $n \cdot e^n = 0$. Pak

$$(n+1)e^{n+1} = \frac{n+1}{n} n \cdot e^n \cdot e \stackrel{\text{IP}}{=} \frac{n+1}{n} \cdot 0 \cdot e = 0.$$

□

Kde je chyba? Z formálního pohledu nám chybí specifikace, pro jaká n potvrzujeme indukční krok. To by nemuselo být fatální, zkusme to doplnit. Algebra při úpravě případu $n+1$ platí pro všechna $n \neq 0$, takže bychom mohli psát například toto:

(1) Pro zvolené $n \in \mathbb{N}$ předpokládejme $n \cdot e^n = 0$. Pak ...

Teď už je zápis v pořádku, ale vidíme, že nám neladí kroky (0) a (1). Máme potvrzenou platnost $V(0)$, takže bychom následně potřebovali implikaci $V(0) \implies V(1)$, ale náš důkaz toto poskytne až od té $V(1) \implies V(2)$. Proto důkaz není platný.

△

Zatímco soulad kroků budeme řešit spíš v dalších sekcích, řada chyb logických či zápisových dokáže pokazit důkaz i v jednoduchých příkladech a trápí zejména začátečníky. Podíváme se na některé oblíbené, abychom se jich vyvarovali.

S 7a.4 Poznámka: Následující chyby jsou mezi začátečníky populární.

1. Také indukce bývá obětí mýtu, že důkaz rovnosti se dělá tak, že si ji napíšeme a pak upravujeme, dokud nedostaneme něco známého. U předchozího příkladu se objevuje třeba toto:

$$\begin{aligned} 1 + 3 + 5 + \dots + (2n+1) &= (n+1)^2 \\ [1 + 3 + 5 + \dots + (2n-1)^2] + (2n+1) &= (n+1)^2 \\ n^2 + (2n+1) &= (n+1)^2 \\ n^2 + 2n + 1 &= n^2 + 2n + 1 \\ 0 &= 0. \end{aligned}$$

Bohužel, toto není důkaz platnosti $V(n+1)$, ale důkaz platnosti rovnosti $0 = 0$ (viz závěr). Používá přitom rovnost $V(n)$ a také $V(n+1)$, takže ony řádky ve skutečnosti dokazují implikaci

$$[V(n) \wedge V(n+1)] \implies 0 = 0.$$

Ta nemá s indukcí nic společného.

V kroku (1) dokazujeme implikaci, tedy platí stejná pravidla jako pro jiné důkazy implikace. Jestliže chceme na základě předpokladů odvodit platnost $V(n+1)$, tak tím cílem rozhodně nesmíme začít, ani to použít někde v průběhu, ale musí se nám to objevit na konci. V tom je jedna z výhod doporučeného přístupu „závěr jako cesta“, nesvádí ke špatné struktuře argumentu.

2. Další oblíbená chyba je vynechat specifikaci, jaká n se vybírají při důkazu implikace v kroku (1). Pak není možné posoudit, zda kroky (0) a (1) na sebe správně navazují, a tedy ani není možné vyhodnotit, zda je důkaz vůbec správně. Je tedy nutně považován za neplatný.

3. S tím souvisí třetí častá chyba, kdy autor důkazu sice rozsah pro n uvede, ale nešikovně, takže vznikne chybná logická struktura. Neformální vyjadřování nemusí být na škodu, ale je třeba hlídat, abychom omylem neřekli něco, co nechceme, popřípadě nevzbudili chybný dojem (zejména u zkoušky toto nechceme).

Nejprve uvedme několik vhodných formulací, které vystihují správný význam indukčního kroku, zejména to, že se implikace dokazuje pro jedno konkrétní zvolené n , formálně

$$\forall n \geq n_0 : [V(n) \implies V(n+1)].$$

Indukční krok (1) lze začít například takto:

- Předpokládejme, že pro jisté libovolně zvolené $n \geq n_0$ platí $V(n)$. Pak ...
- Předpokládejme, že pro dané $n \geq n_0$ platí $V(n)$. Pak ...
- Dáno $n \geq n_0$. Předpoklad: $V(n)$ platí. Pak ...
- Nechť $n \geq n_0$ zvoleno libovolně. Předpokládejme, že platí $V(n)$. Pak ...
- Pro zvolené $n \geq n_0$ předpokládejme platnost $V(n)$. Pak ...
- Zvolme $n \geq n_0$. IP: $V(n)$. Pak ...

Naopak následující formulace jsou nevyhovující:

- Pro $n \geq n_0$ předpokládejme platnost $V(n)$. Pak ...
- Předpokládejme, že pro $n \geq n_0$ platí $V(n)$. Pak ...
- IP: $V(n)$ platí pro $n \geq n_0$. Pak ...

Proč jsou nevhodné? Již jsme se setkali s tím, že matematici se nevyjadřují vždy zcela přesně a existují určité zvyklosti. Jedna z nich je, že tvrzení typu „pro $x \in M$ platí V “ se interpretuje jako „pro všechna $x \in M$ “. Ony

nevhodné formulace by tedy byly chápány jako tvrzení, že se platnost předpokládá $V(n)$ pro všechna n . Formálně se pak vlastně dokazuje

$$[\forall n \geq n_0 : V(n)] \implies V(n+1).$$

To je opět něco jiného, než potřebujeme pro indukci, a navíc to nedává smysl. Pokud bychom předpokládali platnost $V(n)$ pro všechna čísla, tak pak V samozřejmě platí i pro číslo $n+1$ a není co dokazovat.

Je tedy klíčové napsat indukční krok tak, aby bylo zcela zjevné, že se platnost $V(n)$ předpokládá pro přesně jedno konkrétní n vybrané z určitého rozsahu. V tom je podstata indukce, cokoli jiného nebude fungovat.

4. Poslední logická chyba, kterou zde zmíníme, je vzácnější, ale je dobré o ní vědět. Pokud při dokazování platnosti $V(n+1)$ nepoužijeme indukční předpoklad, pak náš důkaz není důkaz indukci, ale nějaký hybrid, který může a nemusí platit. Uvidíme to v příkladě 7a.c.

5. Někteří studenti používají velmi zvláštní formu indukce (bohužel se najde i na Wiki), kdy důkaz strukturují takto:

$$1. n = 1: 1 = 1^2.$$

$$2. n = k: \sum_{i=1}^k (2i - 1) = k^2.$$

$$3. n = k + 1: \text{Důkaz pro případ } k + 1, \text{ dosti často ten chybný pozpátku.}$$

Tento zápis nedává smysl hned ze dvou důvodů. Za prvé, tváří se, že se indukce skládá ze tří kroků, což samozřejmě není pravda. Není žádný důvod dělit důkaz implikace $V(n) \implies V(n+1)$ na nějaké samostatné bloky. Druhým problémem je míchání dvou proměnných. Jedna z nich je evidentně zbytečná. Pokud bychom kroky 2. a 3. interpretovali jako důkaz implikace od k ke $k+1$, pak by pracovní proměnnou mělo být k , což pak ale nesedí s krokem 1. Je to prostě zápis zmatečný a pokud s ním čtenář koketoval, tak velmi silně doporučíme, aby jej rychle opustil.

Tím jsme čtenáře varovali, takže se už snad nedá svést temnou stranou síly a bude produkovat jen správné důkazy.

△

Poznámka: Probrali jsme, co bychom v důkazech indukci dělat neměli, ale jsou modifikace, které jsou v pořádku.

Někteří lidé dokazují indukční krok s posunutým indexem:

- (1) Dáno $n > n_0$. IP: $V(n-1)$ platí. Pak platí $V(n)$.

To je rovnocenné standardnímu postupu. Poskytne totiž sadu implikací

$$V(n_0) \implies V(n_0+1), V(n_0+1) \implies V(n_0+2), V(n_0+2) \implies V(n_0+3), V(n_0+3) \implies V(n_0+4), \text{ atd.}$$

kteřá přesně odpovídá standardnímu kroku (1).

Posun indexu je umožněn tím, že jde o pracovní proměnnou, která je pro krok (1) vnitřní. Mohli bychom tedy místo n použít jiné písmeno, občas se tak potká k . Pak je ale dobré použít stejné písmeno také v kroku (0), protože jde o stejný ukazatel a tyto kroky spolu souvisí.

V tomto spisku se budeme držet tradičního n nikoliv protože bychom museli, ale protože používání zažitého značení usnadňuje srozumitelnost textu.

△

Příklad 7a.c: Ukážeme, že pro $n \geq 0$ je číslo $n^2 + n$ vždy sudé.

Rozbor: Jak budeme pracovat se sudostí? Jedna možnost je pracovat s tímto pojmem intuitivně. Druhá možnost je být striktní a přeložit zadání do jazyka dělitelnosti. Důkaz, že $n^2 + n$ je násobek dvou, je záležitost algebry a tedy formálnější. Ukážeme oba přístupy.

Jaký je vztah mezi situací n a situací $n+1$? Jako obvykle to vezmeme od konce a po dosazení $n+1$ do $n^2 + n$ v tom zkusíme najít původní vzorec s n .

$$(n+1)^2 + (n+1) = n^2 + 2n + 1 + n + 1 = (n^2 + n) + (2n + 2).$$

Povedlo se, jsme připraveni na důkaz. Naše odvození je vlastně začátek hlavní cesty v kroku (1). Začneme verzí povídací.

Dokážeme indukci, že $n^2 + n$ je sudé pro $n \geq 0$.

(0) $n = 0$: $0^2 + 0 = 0$ je sudé.

(1) Dáno $n \geq 0$. IP: $n^2 + n$ je sudé. Pak

$$(n+1)^2 + (n+1) = n^2 + 2n + 1 + n + 1 = (n^2 + n) + (2n + 2).$$

První člen je díky IP sudý, druhý člen $2(n+1)$ je díky $n+1 \in \mathbb{Z}$ také sudý a součet dvou sudých čísel je sudý.

□

Nyní předvedeme algebraickou verzi.

Dokážeme indukci, že pro všechna $n \geq 0$ platí $n^2 + n = 2k$ pro nějaké $k \in \mathbb{Z}$.

(0) $n = 0$: $0^2 + 0 = 0 = 2 \cdot 0$, kde $k = 0 \in \mathbb{Z}$.

(1) Dáno $n \geq 0$. IP: Existuje $k \in \mathbb{Z}$ splňující $n^2 + n = 2k$. Pak

$$(n+1)^2 + (n+1) = n^2 + 2n + 1 + n + 1 = (n^2 + n) + (2n + 2) \stackrel{\text{IP}}{=} 2k + 2(n+1) = 2(k+n+1).$$

Protože $K = k + n + 1 \in \mathbb{Z}$, dokázali jsme, že i $(n+1)^2 + (n+1) = 2K$ pro $K \in \mathbb{Z}$.

□

Třetí verzi důkazu ukážeme v poznámce.

△

Poznámka: Občas se dá potkat také tato verze důkazu:

(0) $n = 0$: $0^2 + 0 = 0$ je sudé.

(1) Dáno $n \geq 0$. IP: $n^2 + n$ je sudé. Pak

$$(n+1)^2 + (n+1) = (n+2)(n+1).$$

Protože jde o dvě po sobě jdoucí celá čísla, jedno z nich musí být sudé a tedy celý součin je sudý.

□

Toto není důkaz indukci, protože v argumentu o případě $n+1$ se vůbec nepoužil indukční předpoklad. Tato chyba se nestává často, ale užitečně nám připomíná, že když přemýšlíme nad případem $n+1$, tak naši primární inspirací je snaha využít IP.

Mimoходом, protože se při zpracování případu $n+1$ došlo k cíli bez použití IP, tak tam vlastně vznikl alternativní, neindukční důkaz. Vypadá takto:

Mějme $n \geq 0$. Protože $n^2 + n = n(n+1)$ je součin dvou po sobě jdoucích celých čísel, musí být jedno z nich sudé a tedy i součin je sudý. Proto je $n^2 + n$ sudé.

Toto je validní důkaz, ale jako odpověď na písemkovou otázku „Dokažte indukci, že ...“ by neuspěl.

△

M 7a.5 Poznámka (indukce a rekurze):

Matematická indukce formálně funguje jako pohyb kupředu, od případu n se přesouváme k případu $n+1$. Ovšem při analýze vztahu těchto dvou situací je přirozenější přemýšlet naopak: Začneme případem $n+1$ a v něm hledáme předchozí situaci n . Tento „zpětný pohled“ je dobře znám programátorům a říká se mu rekurze. Rekurze a inkluze mají tedy stejný základ, nalezení vztahu, jen u rekurze se díváme směrem $(n+1) \mapsto n$, zatímco důkaz indukci postupuje $n \mapsto (n+1)$. V obou případech je vztah stejný, jen jej jinak zpracujeme (program versus důkaz).

△

Poznámka: Indukce je dobrá důkazová technika, ale není odhalovací. Pokud nevíme, kolik je součet n prvních lichých čísel, tak nám s tím nepomůže. Jak se takové výsledky najdou? Například experimentálně. V našem případě můžeme sečíst lichá čísla pro několik n , třeba pro $n = 3$ máme $1 + 3 + 5 = 9$, a když se na výsledky pro různá n přehledně podíváme, tak nás třeba něco napadne.

n :	1	2	3	4	5
\sum :	1	4	9	16	25

Tabulka napovídá vzorec n^2 .

Úspěšnost takového hádání roste s tím, kolik známe populárních posloupností, viz například kapitola 8c. Ale někdy nepomůže ani bohatá zkušenost. Částečné součty harmonické řady

$$H(n) = \sum_{k=1}^n \frac{1}{k} = \frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{n}$$

sice počítat můžeme,

n :	1	2	3	4	5
$H(n)$:	1	$\frac{3}{2}$	$\frac{10}{3}$	$\frac{41}{4}$	$\frac{206}{5}$

ale hádat budeme marně. Je dokázáno, že součty nelze vyjádřit uzavřeným algebraickým vzorcem (zhruba řečeno takovým, do kterého lze přímo dosadit, suma je totiž také vzorec, ale ne uzavřený).

Indukce ale může potvrdit odhady tohoto součtu, viz cvičení 7a.21.

△

Dokazování rovností je v jistém smyslu zrádné, protože je příliš jednoduché. Lépe podstatu indukce rozpoznáme u nerovností.

! **Příklad 7a.d:** Ukážeme indukci, že pro $n \in \mathbb{N}$ platí $2 + 4 + \dots + (2n) > n^2$. Jde tedy o odhad součtu prvních n sudých čísel.

Rozbor: Pro $n + 1$ potřebujeme dokázat $2 + 4 + \dots + 2(n + 1) > (n + 1)^2$. Použijeme metodu cesty, tedy začneme na jedné straně a nabízí se levá. Tam hned vidíme návaznost na předchozí případ:

$$2 + 4 + \dots + 2(n + 1) = [2 + 4 + \dots + (2n)] + 2(n + 1).$$

Důkaz:

(0) $n = 1$: $2 > 1^2$ platí.

(1) Dáno $n \geq 1$, IP: $2 + 4 + \dots + (2n) > n^2$.

Pak

$$\begin{aligned} 2 + 4 + \dots + 2(n + 1) &= [2 + 4 + \dots + (2n)] + 2(n + 1) \\ &\stackrel{\text{IP}}{>} n^2 + 2(n + 1) = n^2 + 2n + 2. \end{aligned}$$

Rozbor: V součtu jsme první člen nahradili něčím, co je podle IP menší; Pak se celý součet zmenší a máme tedy právo napsat to $\dots > n^2 + 2n + 2$.

Teď ale máme problém, nedostali jsme správný výraz pro pravou stranu. To ale neznamená, že je indukce špatně, jen jsme rozmazlení snadným případem rovnosti a tohle nás zaskočilo.

Naším cílem je dostat se od levé strany k pravé s tím, že ta pravá má být menší. Zatím jsme ukázali, že levá strana je větší než jeden nechtěný výraz. Pokud ukážeme, že tento nechtěný výraz je větší či roven $(n + 1)^2$, tak to spojíme a dostaneme to, co potřebujeme. Jedna možnost je dokázat jako samostatný blok, že $n^2 + 2n + 2 > (n + 1)^2$. Ve složitějších případech to je dokonce vhodné. U jednodušších se nabízí pokračovat v započaté cestě a výraz ještě vhodně zmenšit. Umíme odhadnout jak, protože víme, kam se chceme trefit. Zkusme to znovu:

Pak

$$\begin{aligned} 2 + 4 + \dots + 2(n + 1) &= [2 + 4 + \dots + (2n)] + 2(n + 1) \\ &\stackrel{\text{IP}}{>} n^2 + 2(n + 1) = n^2 + 2n + 2 > n^2 + 2n + 1 = \underline{(n + 1)^2}. \end{aligned}$$

□

U té druhé nerovnosti se použil fakt, že $2 > 1$, což jistě platí. Je dobrým zvykem čtenáře upozornit, na základě čeho výrazy upravujeme, možný zápis ukážeme v dalším příkladě.

Mimoходом, hodnotu součtu sudých čísel lze najít pomocí známého vzorce pro součet prvních n přirozených čísel (jehož potvrzení je asi nejprofláklejší příklad na indukci).

$$2 + 4 + \dots + (2n) = 2(1 + 2 + \dots + n) = 2 \cdot \frac{1}{2}n(n + 1) = n(n + 1).$$

To občas svádí k následujícímu pokusu o důkaz (použijeme sumační značení, ať jej také vidíme v akci).

(0) $n = 1$: $\sum_{k=1}^1 (2k) = 2 > 1^2$ platí.

(1) Dáno $n \geq 1$, IP: $\sum_{k=1}^n (2k) > n^2$.

Pak

$$\sum_{k=1}^{n+1} (2k) = 2 \sum_{k=1}^{n+1} k = 2 \cdot \frac{1}{2}(n + 1)(n + 1 + 1) = (n + 1)(n + 2) \geq (n + 1)^2.$$

□

Čtenář jistě rozpoznal problém: Indukční předpoklad se nikde nepoužil, tedy nejde o důkaz indukci.

△

S 7a.6 Poznámka: V důkazu indukčního kroku lze také postupovat úpravami předpokladu, dokud nezískáme závěr.

$$\begin{aligned} \text{IP: } \quad \sum_{k=1}^n (2k) &\geq n^2 & / & + (2n + 2) \\ \sum_{k=1}^n (2k) + 2(n + 1) &\geq n^2 + 2n + 2 \\ \sum_{k=1}^{n+1} (2k) &\geq (n^2 + 2n + 1) + 1 \\ \sum_{k=1}^{n+1} (2k) &\geq (n + 1)^2 + 1 & / & 1 > 0 \end{aligned}$$

$$\sum_{k=1}^{n+1} (2k) \geq (n+1)^2.$$

V poslední kroku jsme vynecháním kladného čísla pravou stranu ještě více zmenšili, tedy nová nerovnost platí, pokud platí i ta předchozí.

Tento postup je korektní, ale ve srovnání s přístupem přes řetízek nerovností delší a pro čtenáře může být obtížnější zdůvodňování jednotlivých kroků.

V tom je jedna z výhod používání řetízků rovností a nerovností. Intuitivně, každá rovnost či nerovnost reprezentuje přechod od „starého“ výrazu k „novému“ a změny jsou snadno posouditelné. Pokud například nahradíme část součtu něčím větším, tak se celek zvětší.

Formálně: Uvažujme čísla či výrazy a, b a také B . Předpokládejme, že $b < B$. Přičtením a dokážeme, že platí $a + b < a + B$, ale lze to také čtením zleva doprava coby součást řetízku úprav interpretovat tak, že když od součtu $a + b$ přejdeme k $a + B$, tak se celek zvětší. Podobně snadno dokážeme, že pokud $a > 0$, tak máme $ab < aB$. Ovšem pozor, $a - b > a - B$ (odečítáme víc, tedy nový výraz se zmenší).

Pro úplnost se vraťme k chybnému přístupu k dokazování směrem od konce. Víme, že je to logicky špatně, ale u nerovností je dokonce problém i s algebra samotnou. Začali bychom takto:

$$\sum_{k=1}^{n+1} (2k) \geq (n+1)^2$$

$$\sum_{k=1}^n (2k) + 2(n+1) \geq n^2 + 2n + 1$$

Nyní bychom rádi aplikovali IP, ale není jak. Říká nám, že sumu lze nahradit výrazem n^2 s tím, že může dojít ke zmenšení. Ovšem zmenšením se levá strana, která byla původně větší, může stát menší než ta pravá. A nebo také ne. My prostě nevíme a pokud nahradíme sumu podle IP menším výrazem, tak nová levá a pravá strana mohou mít jakýkoliv vztah, konec cesty.

△

Příklad 7a.e: Dokážeme, že pro $n \in \mathbb{N}_0$ platí $n < 2^n$.

Rozbor: Případ $n + 1$ neboli nerovnost $n + 1 < 2^{n+1}$ dokážeme postupným přechodem od jedné strany ke druhé. Začneme na levé straně a zkusíme se propracovat k pravé, kde se hodí pozorování $2^{n+1} = 2 \cdot 2^n = 2^n + 2^n$. Opět bude třeba trochu kouzlit a čtenáře na použitý chvat upozorníme v poznámce.

V základním kroku máme ověřit platnost $0 < 2^0$ neboli $0 < 1$, což platí. Musíme to ovšem nějak napsat a metoda cesty opět nabízí efektivní zápis.

(0) $n = 0$: Platí $0 < 1 = 2^0$.

(1) Dáno $n \in \mathbb{N}_0$, IP: $n < 2^n$.

Pak

$$\frac{n+1}{\leq 2^n + 2^n = 2^{n+1}} < 2^n + 1 \quad \Bigg/ \quad n \geq 0 \implies 1 \leq 2^n$$

□

Kroky lze otočit a dostaneme rovněž správný důkaz:

$$2^{n+1} = 2^n + 2^n \stackrel{\text{IP}}{>} n + 2^n \geq n + 1. \quad \Bigg/ \quad n \geq 0 \implies 2^n \geq 1.$$

Indukční předpoklad jsme použili jednou, ale můžeme jej použít dvakrát a nahradit obě 2^n . Pak dostaneme

$$2^{n+1} = 2^n + 2^n \stackrel{\text{IP}}{>} n + n = 2n.$$

Potřebovali bychom v dalším kroku přejít $2n \geq n + 1$, ale to platí jen pro $n \geq 1$, nikoliv pro $n = 0$, kde to také potřebujeme pro správnou návaznost kroků v indukci. Stejný zádrhel nastane, když místo sčítání použijeme násobení:

$$2^{n+1} = 2 \cdot 2^n \stackrel{\text{IP}}{>} 2 \cdot n.$$

Problém není v indukci ani v implikaci, tu jsme ostatně již dvakrát dokázali, ale v riziku spojeném s prací s nerovnostmi. U každé nerovnosti něco ztrácíme a je potřeba, abychom dohromady nepoztráceli moc, což se nám teď bohužel stalo. Nerovnost $2^n > n$ v IP znamená jistou ztrátu. Když ji aplikujeme jednou, tak si ztrátu můžeme dovolit. Ale když IP použijeme dvakrát, tak jsme také ztratili dvakrát a to už je moc. V některých situacích by to nevadilo a rozklad $a^{n+1} = a^n \cdot a$ je v indukčních důkazech populární, ale zde to nevyšlo.

Obdobnou situaci lze potkat ve cvičení 7a.20, ale běžné to (naštěstí) není.

△

Ne vždy je nalezení vztahu mezi případy n a $n + 1$ snadné. Mnohdy pomůže podívat se na několik konkrétních situací.

Příklad 7a.f: Podíváme se na součet

$$s_n = \sum_{k=n}^{2n} k = n + (n + 1) + \cdots + (2n).$$

Jak tyto součty vypadají?

$$s_3 = 1 + 2$$

$$s_4 = 2 + 3 + 4$$

$$s_5 = 3 + 4 + 5 + 6.$$

Máme tedy následující:

$n:$	1	2	3	4	5
$s_n:$	3	9	18	30	45

To nevypadá jako nějaký jednoduchý vzorec. Možná čtenáře napadne, ale my se spokojíme s něčím, co je vidět hned, například $s_n > n^2$. Dokážeme to indukcí pro $n \geq 1$.

Rozbor: Potřebujeme najít vztah mezi s_n a s_{n+1} . Spočítané příklady výše ukazují, že při přechodu od s_n k s_{n+1} zmizí první číslo a na konci přibudou dvě navíc, tedy

$$\begin{aligned} s_{n+1} &= \sum_{k=n+1}^{2n+2} k = [(n+1) + \cdots + (2n)] + (2n+1) + (2n+2) \\ &= s_n - n + (2n+1) + (2n+2). \end{aligned}$$

Jsme připraveni.

$$(0) \ n = 1: \underline{s_1} = 3 > 1 = \underline{1^2}.$$

$$(1) \ \text{Dáno } n \geq 1, \text{ IP: } s_n > n^2. \text{ Dokážeme, že pak } s_{n+1} > (n+1)^2:$$

$$\begin{aligned} \underline{s_{n+1}} &= s_n - n + (2n+1) + (2n+2) \stackrel{\text{IP}}{>} n^2 - n + (2n+1) + (2n+2) = n^2 + 3n + 3 \\ &= (n^2 + 2n + 1) + (n+2) \quad / \quad n \geq 1 \implies n+2 > 0 \\ &> n^2 + 2n + 1 = \underline{(n+1)^2}. \end{aligned}$$

□

Čitelnosti napomohla poznámka a také to, že jsme nejprve výraz $n^2 + 3n + 3$ připravili tak, ať je v něm vidět cíl $n^2 + 2n + 1$, takže bylo jasné, co je tam navíc. Dalo by se ovšem také argumentovat tak, že pro $n \geq 1$ platí $3n > n$ a $3 > 1$, a proto $n^2 + 3n + 1 > n^2 + 2n + 1$ (dvojnásobek zmenšení najednou).

Dolní odhad je pěkný, ale přece jenom bychom raději přesnou hodnotu. Z tabulky jsme ji možná neuhodli, ale čtenář nejspíše zná vzorec pro součet prvních n přirozených čísel. Pomocí něj odvodíme

$$\begin{aligned} s_n &= \sum_{k=n}^{2n} k = \sum_{k=1}^{2n} k - \sum_{k=1}^{n-1} k \\ &= \frac{1}{2}(2n)(2n+1) - \frac{1}{2}(n-1)(n-1+1) = \frac{1}{2}(4n^2 + 2n - n^2 + n) = \frac{3}{2}n(n+1). \end{aligned}$$

I toto se snadno dokáže indukcí. Nejprve se ale vyplatí si rozmyslet, že pro $n+1$ se pravá strana rovná

$$\frac{3}{2}(n+1)((n+1)+1) = \frac{3}{2}(n+1)(n+2) = \frac{3}{2}(n^2 + 3n + 2).$$

Teď víme, kam míříme.

$$(0) \ n = 1: \underline{s_1} = 3 = \frac{3}{2} \cdot 1 \cdot (1+1).$$

$$(1) \ \text{Dáno } n \geq 1, \text{ IP: } s_n = \frac{3}{2}n(n+1). \text{ Dokážeme, že pak } s_{n+1} = \frac{3}{2}(n+1)(n+2):$$

$$\begin{aligned} \underline{s_{n+1}} &= s_n - n + (2n+1) + (2n+2) \stackrel{\text{IP}}{=} \frac{3}{2}n(n+1) - n + (2n+1) + (2n+2) = \frac{3}{2}n(n+1) + 3n + 3 \\ &= \frac{3}{2}(n^2 + n) + \frac{3}{2}(2n+2) = \frac{3}{2}(n^2 + 3n + 2) = \underline{\frac{3}{2}(n+1)(n+2)}. \end{aligned}$$

□

Jako obvykle nám u rovnosti vyšel přímo správný výraz.

△

Podívejme se ještě na dvě nerovnosti.

! Příklad 7a.g: Dokážeme, že pro každé $n \in \mathbb{N}$, $n \geq 3$ platí $n^2 > n + 5$.

Rozbor: Krok (1) dokážeme doporučenou metodou cesty. Levá strana vypadá komplikovaněji, tak s ní začneme, potřebujeme se tedy od $(n+1)^2$ dostat k výrazu $(n+1) + 5 = n + 6$. Příklad $n+1$ se na případ n převede snadno.

V kroku (0) chceme ukázat, že $3^2 > 3 + 5$ neboli $9 > 8$. Ověření se opět nejlépe zapíše pomocí cesty.

(0) $n = 3$: platí $3^2 = 9 > 8 = 3 + 5$.

(1) Dáno $n \geq 3$, pro něj předpokládejme, že $n^2 > n + 5$. (IP)

Pak platí

$$\begin{aligned} \underline{(n+1)^2} &= n^2 + 2n + 1 \stackrel{\text{IP}}{>} (n+5) + 2n + 1 = (n+6) + 2n & / \quad n \geq 3 \implies 2n > 0 \\ &> n + 6 + 0 = \underline{(n+1) + 5}. \end{aligned}$$

□

Všimneme si, že úprava $2n > 0$, která nám umožnila dokončit důkaz, je ve skutečnosti platná pro $n \geq 1$. To znamená, že implikace $V(n) \implies V(n+1)$ platí pro všechna $n \in \mathbb{N}$. Jinak řečeno, jsme schopni správně rozestavit domina počínaje tím s číslem 1. Problém ale je, že několik prvních domin nejsme schopni shodit neboli nejsme schopni provést krok (0) pro menší n než 3. Proto je potřeba začít důkaz indukčního kroku (1) až od trojky, aby navazoval na základní krok, ačkoliv platí i dříve.

△

Příklad 7a.h: Dokážeme, že pro $n \geq -3$ platí $n \leq n^2$.

Rozbor: Příklad $n+1$ neboli nerovnost $n+1 \leq (n+1)^2$ dokážeme postupným přechodem od jedné strany ke druhé. Začneme druhou mocninou, protože vypadá komplikovaněji. Abychom nemátli čtenáře změnou směru uprostřed důkazu, budeme dokazovat $n^2 \geq n$.

(0) $n = -3$: Platí $(-3)^2 = 9 \geq -3$.

(1) Dáno $n \geq -3$, IP: $n^2 \geq n$.

Pak

$$\underline{(n+1)^2} = n^2 + 2n + 1 \stackrel{\text{IP}}{>} n + 2n + 1 = (n+1) + 2n.$$

Máme problém. Potřebovali bychom cestu dokončit krokem $(n+1) + 2n \geq n+1$, ale ten platí pouze pro $n \geq 0$, nikoliv pro $n \geq -3$. Bohužel, potřebná implikace se nedá dokázat algebrou obecně pro $n \geq -3$.

Co s tím uděláme? Tvrzení rozdělíme na dva případy. Pro čísla $n = -3, -2, -1$ nerovnost ověříme přímo (necháme čtenáři) a pro $n \geq 0$ použijeme indukci:

(0) $n = 0$: $0^2 \geq 0$ platí.

(1) Dáno $n \geq 0$, IP: $n^2 \geq n$.

Pak

$$\begin{aligned} \underline{(n+1)^2} &= n^2 + 2n + 1 \stackrel{\text{IP}}{\geq} n + 2n + 1 = (n+1) + 2n & / \quad n \geq 0 \implies 2n \geq 0 \\ &\geq \underline{n+1}. \end{aligned}$$

□

Tentokrát umíme shazovat domina už pro záporná čísla, ale správně je rozestavit umíme až od čísla 0. Vidíme, že někdy musíme základní a indukční kroky sladit.

△

Příklad 7a.i: Víme, že pro $n \in \mathbb{N}$ platí $1 < \frac{n+1}{n} \leq 2$. Dokáže se to snadno například pomocí přepisu $\frac{n+1}{n} = 1 + \frac{1}{n}$, ale my se to pokusíme ukázat indukcí.

Rozbor: Zjistíme, čím se případ $n+1$ liší od případu n . Nabízí se dvě možnosti, pomocí násobení a sčítání.

$$\begin{aligned} \frac{(n+1)+1}{n+1} &= \frac{n+2}{n+1} = \frac{n+1}{n} \cdot \frac{n(n+2)}{(n+1)^2}, \\ \frac{(n+1)+1}{n+1} &= 1 + \frac{1}{n+1} = 1 + \frac{1}{n} + \frac{1}{n+1} - \frac{1}{n} = \frac{n+1}{n} - \frac{1}{(n+1)n}. \end{aligned}$$

Pokud bychom použili první verzi, pak bychom se museli ptát na velikost toho druhého zlomku napravo, takže bychom přešli od daného problému k obdobnému, dokonce komplikovanějšímu. Proto dává víc smyslu použít druhý přepis, kde hned vidíme, že $\frac{1}{n(n+1)} > 0$ pro $n \in \mathbb{N}$. Nejprve dokážeme horní odhad:

(0) $n = 1$: $\frac{1+1}{1} = 2 \leq 2$ platí.

(1) Dáno $n \in \mathbb{N}$, IP: $\frac{n+1}{n} \leq 2$. Pak díky $\frac{1}{n(n+1)} > 0$ máme

$$\underline{\frac{n+2}{n+1}} = \frac{n+1}{n} - \frac{1}{n(n+1)} < \frac{n+1}{n} \stackrel{\text{IP}}{\leq} 2.$$

□

Vyšlo to. Nyní zkusíme dolní odhad.

(0) $n = 1$: $\frac{1+1}{1} = 2 > \underline{1}$ platí.

(1) Dáno $n \in \mathbb{N}$, IP: $\frac{n+1}{n} > 1$. Pak máme

$$\frac{n+2}{n+1} = \frac{n+1}{n} - \frac{1}{n(n+1)} \stackrel{\text{IP}}{>} 1 - \frac{1}{n(n+1)}$$

Máme problém. Potřebovali bychom navázat nerovností ≥ 1 , ale to zjevně není pravda pro žádné n . Potřebnou implikaci tedy v této podobě nedokážeme dokázat.

△

Příklad ukazuje, že ne každé tvrzení týkající se situací popsaných celými čísly, kdy existuje vztah mezi případy n a $n+1$, je dokazatelné indukcí. Ten vztah musí být také pro indukci vhodný. Problémy nastávají zřídka (viz cvičení 7a.22) a určitě nenastanou u rovností.

Na druhou stranu je indukce docela flexibilní a lze ji aplikovat také na jiné situace než rovnosti a nerovnosti. Pro zvědavého čtenáře jsme zařadili bonusovou sekci s příklady. Je také možné indukcí dokázat, že nějaké tvrzení nikdy neplatí, indukčním důkazem platnosti jeho negace.

7a.7 Indukce a definice

Občas se zde vyjadřujeme nepříliš pochvalně o třech tečkách, které jsou sice nápomocné naší intuici, ale nedá se s nimi přesně pracovat. Typickým případem je výraz $2 + 3 + \dots + 23$. Obsahuje ten součet třináctku nebo ne? Intuitivně ano, ale umíme to dokázat?

Ve snaze o přesnost jsme přecházeli k sumačnímu značení a v důkazech indukcí využívali užitečnou identitu, ale co vlastně suma znamená? Odpověď dá indukce, která také umí vytvářet nové objekty.

Definice.

Nechť $n_0 \in \mathbb{Z}$. Uvažujme čísla $a_k \in \mathbb{R}$ pro $k \in \mathbb{Z}$, $k \geq n_0$. Jejich součty definujeme takto:

$$(0) \sum_{k=n_0}^{n_0} a_k = a_{n_0};$$

$$(1) \sum_{k=n_0}^{n+1} a_k = \sum_{k=n_0}^n a_k + a_{n+1} \quad \text{pro } n \in \mathbb{Z}, n \geq n_0.$$

Jejich součiny definujeme takto:

$$(0) \prod_{k=n_0}^{n_0} a_k = a_{n_0};$$

$$(1) \prod_{k=n_0}^{n+1} a_k = \left(\prod_{k=n_0}^n a_k \right) \cdot a_{n+1} \quad \text{pro } n \in \mathbb{Z}, n \geq n_0.$$

Někdy se také pro úplnost definuje $\sum_{k=n_0}^n a_k = 0$ a $\prod_{k=n_0}^n a_k = 1$ pro $n < n_0$.

Jak víme, že tím něco vzniklo? Intuitivně je to jasné, ukažme to pro oblíbený případ $n_0 = 1$. Podle (0) umíme $\sum_{k=1}^1 a_k = a_1$, tak to chceme. Následuje suma $\sum_{k=1}^2 a_k$, se kterou nám pomůže specifikace (1) díky $\sum_{k=1}^2 a_k = \sum_{k=1}^{1+1} a_k$, tedy potřebujeme použít (1) s volbou $n = 1$. Protože jsme (1) specifikovali pro $n \geq n_0 = 1$, máme vzorec k dispozici. Říká, že

$$\sum_{k=1}^2 a_k = \sum_{k=1}^{1+1} a_k \stackrel{(1)}{=} \sum_{k=1}^1 a_k + a_{1+1}.$$

Tu sumu napravo již známe z kroku (0), je tedy vidět, že specifikace (0) a (1) jsou dobře sladěny. Dostáváme

$$\sum_{k=1}^2 a_k = \sum_{k=1}^{1+1} a_k \stackrel{(1)}{=} \sum_{k=1}^1 a_k + a_{1+1} = a_1 + a_2.$$

Díky této znalosti pak pomocí (1) s volbou $n = 2$ získáme obdobně $\sum_{k=1}^3 a_k = a_1 + a_2 + a_3$ atd.

Definice tedy zdá se funguje, jistotu nám dá důkaz indukci. Tvrdíme, že pokud máme čísla a_k , $k \in \mathbb{Z}$, $k \geq n_0$, pak pro všechna $n \geq n_0$ je $\sum_{k=1}^n a_k$ korektně definováno a představuje jisté konkrétní číslo.

Při práci s objekty vzniklými indukcí či rekurzí netřeba vztah mezi případy n a $n+1$ hledat, protože jej máme přímo v definici (1).

(0) $n = n_0$: Podle definice existuje $\sum_{k=1}^{n_0} a_k = a_{n_0}$, což je konkrétní číslo.

(1) Pro dané $n \geq n_0$ předpokládejme, že symbol $\sum_{k=n_0}^n a_k$ je korektně definován a značí konkrétní číslo, označme

jej A . Pak je také $A + a_{n+1}$ existující konkrétní číslo a proto je symbol $\sum_{k=n_0}^{n+1} a_k \stackrel{(1)}{=} \sum_{k=n_0}^n a_k + a_{n+1}$ korektně definován a značí konkrétní číslo.

□

Důkaz pro součin je obdobný.

Příklad 7a.j: Zajímavým typem sum jsou „teleskopické sumy“, klasickým příkladem je $\sum_{k=1}^n \frac{1}{k(k+1)}$. Zrovna tato je ale maskovaná, teleskopování uvidíme, když členy vhodně přepíšeme.

$$\sum_{k=1}^n \frac{1}{k(k+1)} = \sum_{k=1}^n \left(\frac{1}{k} - \frac{1}{k+1} \right) = \left(1 - \frac{1}{2} \right) + \left(\frac{1}{2} - \frac{1}{3} \right) + \left(\frac{1}{3} - \frac{1}{4} \right) + \cdots + \left(\frac{1}{n-1} - \frac{1}{n} \right) + \left(\frac{1}{n} - \frac{1}{n+1} \right).$$

Intuice nám říká, že všechny prostřední zlomky se navzájem vyruší a suma se tak zaklapne jako pirátský dalekohled. Matematicky řečeno,

$$\sum_{k=1}^n \left(\frac{1}{k} - \frac{1}{k+1} \right) = 1 - \frac{1}{n+1}.$$

Ovšem tři tečky a pocit nejsou korektní matematika, tak to dokážeme indukcí pro $n \in \mathbb{N}$.

(0) $n = 1$: $\sum_{k=1}^1 \left(\frac{1}{k} - \frac{1}{k+1} \right) = \frac{1}{1} - \frac{1}{2} = 1 - \frac{1}{1+1}$.

(1) Zvoleno $n \in \mathbb{N}$, IP: $\sum_{k=1}^n \left(\frac{1}{k} - \frac{1}{k+1} \right) = 1 - \frac{1}{n+1}$. Pak

$$\begin{aligned} \sum_{k=1}^{n+1} \left(\frac{1}{k} - \frac{1}{k+1} \right) &= \sum_{k=1}^n \left(\frac{1}{k} - \frac{1}{k+1} \right) + \left(\frac{1}{n+1} - \frac{1}{n+2} \right) \\ &\stackrel{\text{IP}}{=} \left(1 - \frac{1}{n+1} \right) + \left(\frac{1}{n+1} - \frac{1}{n+2} \right) = 1 - \frac{1}{(n+1)+1}. \end{aligned}$$

□

Intuice je potvrzena.

△

Jakýkoliv matematický zápis zahrnující tři tečky v sobě schovává definici pomocí indukce. Vedle sum se to týká zejména mocnin, které definujeme následovně.

Definice.

Uvažujme číslo $a \in \mathbb{R}$. Jeho mocniny definujeme takto:

(0) $a^0 = 1$;

(1) $a^{n+1} = a^n \cdot a$ pro $n \in \mathbb{N}_0$.

Když máme mocninu korektně definovanu, můžeme o ní dokazovat hluboké poznatky, třeba tento.

Příklad 7a.k: Dokážeme indukcí, že $1^n = 1$ pro $n \in \mathbb{N}_0$.

(0) $n = 0$: $1^0 = 1$ dle specifikace (0) v definici mocniny.

(1) Dáno $n \geq 0$, IP: $1^n = 1$.

Pak podle specifikace (1) v definici mocniny platí

$$\underline{1^{n+1}} = 1^n \cdot 1 \stackrel{\text{IP}}{=} 1 \cdot 1 = \underline{1}.$$

□

Toto byl samozřejmě pokus o matematický vtíp, nicméně čtenář by si měl všimnout, jak korektně vytváříme důkaz indukci, který mimochodem svou strukturou následuje strukturu definice mocniny. Jak uvidíme později, není to náhoda.

△

V situaci, kdy něco definujeme indukcí a také o tom něco indukcí dokazujeme, se potřebujeme vyznat, které (0) a (1) je které. Abychom pořad nemuseli psát „(0) z definice“, budeme v takových situacích pro rozlišení používat u definic (0_D) a (1_D) .

Jedním z nejpůvodnějších objektů vytvářených indukcí je faktoriál.

Definice.

Funkci **faktoriál** značenou $n!$ definujeme pro $n \in \mathbb{N}_0$ takto:

(0_D) $0! = 1$;

(1_D) $(n+1)! = (n+1) \cdot n!$ pro $n \in \mathbb{N}_0$.

Opakovaným použitím předpisu (1_D) pro $n = 0$, pak $n = 1$ atd. zjistíme, že $1! = 1 \cdot 0! = 1 \cdot 1 = 1$, $2! = 2 \cdot 1! = 2 \cdot 1$, $3! = 3 \cdot 2! = 3 \cdot 2 \cdot 1$, $4! = 4 \cdot 3! = 4 \cdot 3 \cdot 2 \cdot 1$ a tak dále, třítečkový zápis je zde výmluvný a obvykle se preferuje jít od 1 k větším číslům:

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n.$$

Potvrdíme, že jsme funkci faktoriál vytvořili, a také dokážeme, že roste velmi rychle.

Příklad 7a.l: Dokážeme, že pro $n \in \mathbb{N}_0$ číslo $n!$ existuje.

(0) $n = 0$: Podle (0_D) číslo $0!$ existuje.

(1) Dáno $n \geq 0$. IP: Číslo $n!$ existuje. Pak také existuje číslo $(n+1) \cdot n!$, tedy podle (1_D) existuje $(n+1)!$

□

Teď dokážeme, že pro $n \geq 4$ platí $n! > 2^n$.

(0) $n = 4$: Platí $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24 > 16 = 2^4$.

(1) Dáno $n \geq 4$. IP: $n! \geq 2^n$. Pak

$$\begin{aligned} \frac{(n+1)!}{n!} &= \frac{(n+1) \cdot n!}{n!} \stackrel{\text{IP}}{>} (n+1) \cdot 2^n & / \quad n \geq 4 \implies (n+1) \geq 2 \\ &\geq 2 \cdot 2^n = 2^{n+1}. \end{aligned}$$

□

Indukční krok by šlo dokázat už pro $n \geq 1$, ale bylo by to zbytečné, protože žádaná nerovnost pro $n = 0, 1, 2, 3$ neplatí.

Faktoriál býval velmi populární mezi uživateli kalkulaček. Roste tak rychle, že kalkulačky 20. století nedokázaly spočítat $70!$, dokonce i mnohé moderní kalkulátory to nezvládnou.

△

Obdobně můžeme pracovat také s jinými funkcemi.

Příklad 7a.m: Uvažujme funkci definovanou na \mathbb{N}_0 následovně:

(0_D) $f(0) = 13$;

(1_D) $f(n+1) = f(n) \cdot 3$ pro $n \geq 0$.

Abychom se ujistili, že na sebe základní a indukční krok správně navazují, spočítáme několik prvních hodnot:

$$\begin{aligned} f(0) &\stackrel{(0_D)}{=} 13, \\ f(1) &= f(0+1) \stackrel{(1_D)}{=}_{n=0} f(0) \cdot 3 = 13 \cdot 3 = 39, \\ f(2) &= f(1+1) \stackrel{(1_D)}{=}_{n=1} f(1) \cdot 3 = 39 \cdot 3 = 117, \\ f(3) &= f(2+1) \stackrel{(1_D)}{=}_{n=2} f(2) \cdot 3 = 117 \cdot 3 = 351, \dots \end{aligned}$$

Zdá se, že nám to správně funguje. Mohli bychom zase dokázat indukcí, že $f(n)$ existuje pro $n \in \mathbb{N}_0$, ale zajímavější bude zjistit něco o jejích hodnotách. Výsledná čísla se nepodobají nějaké populární posloupnosti, takže možná nevidíme vzorečkový vztah mezi n a $f(n)$ (tzv. explicitní vzorec pro f), ale můžeme si všimnout, že hodnoty $f(n)$ jsou vždy větší než odpovídající mocnina dvojky (ty dobře známe).

Dokážeme indukcí, že $f(n) > 2^n$ pro $n \in \mathbb{N}_0$. Přejít mezi případy $f(n+1)$ a $f(n)$ nám zajistí specifikace (1_D) .

(0) $n = 0$: platí $f(0) \stackrel{(0_D)}{=} 13 > 1 = 2^0$.

(1) Pro zvolené $n \geq 0$ předpokládejme $f(n) > 2^n$. Pak

$$\begin{aligned} \frac{f(n+1)}{f(n)} &\stackrel{(1_D)}{=} f(n) \cdot 3 \stackrel{\text{IP}}{>} 2^n \cdot 3 & / \quad 3 > 2 \\ &> 2^n \cdot 2 = 2^{n+1}. \end{aligned}$$

□

Pokud bychom chtěli mít šanci uhodnout přesný vzorec, pak je lepší při experimentování čísla nespojovat v jeden výsledek, ale nechávat jednotlivé složky, abychom viděli, jak se nám hodnoty vytvářejí.

$$\begin{aligned} f(0) &\stackrel{(0_D)}{=} 13, \\ f(1) &= f(0+1) \stackrel{(1_D)}{=} f(0) \cdot 3 = 13 \cdot 3, \\ f(2) &= f(1+1) \stackrel{(1_D)}{=} f(1) \cdot 3 = 13 \cdot 3 \cdot 3, \\ f(3) &= f(2+1) \stackrel{(1_D)}{=} f(2) \cdot 3 = 13 \cdot 3 \cdot 3 \cdot 3 = 13 \cdot 3^3, \\ f(4) &= f(3+1) \stackrel{(1_D)}{=} f(3) \cdot 3 = 13 \cdot 3^3 \cdot 3 = 13 \cdot 3^4, \dots \end{aligned}$$

Optimista by si tipnul, že $f(n) = 13 \cdot 3^n$, například $f(0) = 13 = 13 \cdot 3^0$ také souhlasí.

Dokážeme indukcí, že $f(n) = 13 \cdot 3^n$ pro $n \in \mathbb{N}_0$.

(0) $n = 0$: platí $f(0) \stackrel{(0_D)}{=} 13 = 13 \cdot 3^0$.

(1) Pro zvolené $n \geq 0$ předpokládejme, že $f(n) = 13 \cdot 3^n$. Pak

$$f(n+1) \stackrel{(1_D)}{=} f(n) \cdot 3 \stackrel{IP}{=} 13 \cdot 3^n \cdot 3 = 13 \cdot 3^{n+1}.$$

□

Důkaz je hotov. Další podobné příklady viz cvičení, pokročilejší verzi potkáme v další sekci.

△

Funkce či posloupnosti definované induktivně vznikají často v situacích, které řešíme rekurzí.

Příklad 7a.n: Představme si, že potřebujeme pověsit záclonu či závěs na háčky, přičemž bychom chtěli, aby byly rozmístěny pokud možno rovnoměrně. Na to je dobrá metoda bisekce neboli půlení.

Nejprve pověsíme na krajní háčky levý a pravý konec závěsu. Ten se pak prověsí a je snadné najít střed, který zavěšíme. Tím jsme původní oblouk rozdělili na poloviny s dobrou přesností. Vznikly tak dva prověsy, u kterých zase snadno najdeme středy a zavěšíme.



Takto pokračujeme, dokud nepoužijeme všechny háčky. Má to ovšem háček, tento způsob funguje pouze v případech, kdy je vhodný počet háčků. Například čtyři háčky tímto způsobem nerozmístíme. Což nás přivádí k otázce: Jaké počty háčků je možné rozmístit metodou bisekce?

Postup rozdělíme do etap a jako t_n označíme počet háčků, které jsou připevněny po etapě číslo n . Začneme nultou etapou neboli zavěšením levého a pravého okraje, takže $t_0 = 2$. Jak jsme viděli, $t_1 = 3$ a $t_2 = 5$. Jak je to obecně? Na konci každé etapy je t_n rovnoměrně rozmístěných háčků, mezi kterými tak vznikne $t_n - 1$ oblouků. Každý z nich přidá nový háček, proto

$$t_{n+1} = t_n + (t_n - 1) = 2t_n - 1.$$

Dostali jsme rekurentní vztah, který můžeme požit jako indukční k vygenerování hledané posloupnosti. Máme $t_3 = 9$, $t_4 = 17$, $t_5 = 33$, $t_6 = 65$. Vypadá to, že $t_n = 2^n + 1$. Potvrdíme indukcí.

(0) $n = 0$: Platí $t_0 = 2 = 2^0 + 1$.

(1) Dáno $n \geq 0$, předpokládejme, že pro něj platí $t_n = 2^n + 1$. Pak

$$t_{n+1} = 2t_n - 1 \stackrel{IP}{=} 2 \cdot (2^n + 1) - 1 = 2 \cdot 2^n + 2 - 1 = 2^{n+1} + 1.$$

□

Zjistili jsme, že bisekcí umíme rozvěsit $2^n + 1$ háčků. K tomuto výsledku se lze dostat snáze tak, že se zaměříme nikoliv na háčky, ale na vzniklé úseky. Je zjevné, že jejich počet je o jedno nižší než počet háčků, a dlouholetá zkušenost nám říká, že když potřebujeme například tabulku rozdělit rovnoměrně na více sloupců, tak to nejlépe funguje půlením pro počty sloupců ve tvaru 2^n . To bychom se ale připravili o zábavu výše.

△

V této sekci jsme připomněli jednoduchou verzi indukce, která je nicméně velmi silným nástrojem v řadě oblastí matematiky. Viděli jsme, jak pomocí ní dokážeme rozšířit sčítání a násobení ze dvou složek na libovolný (konečný) počet zavedením pojmu sumy a mocniny. Obdobně jsme v kapitole o relacích zavedli skládání a mocninu relace, popřípadě pomocí zobecnili tranzitivní situaci z dvojkroků na více kroky. Některé z těchto výsledků připomeneme ve cvičeních.

Cvičení

Cvičení 7a.1 (rutinní, poučné): Dokažte pro $n \in \mathbb{N}$ následující fakta. Pokaždé sestavte tři důkazy, a to s použitím třítečkového, sumačního a algebraického značení. Protože jde o jednoduchá tvrzení, soustřeďte se na správnou strukturu důkazu a zápis.

$$\text{a) } \underbrace{0 + 0 + \cdots + 0}_n = \sum_{k=1}^n 0 = n \cdot 0 = 0;$$

$$\text{c) } \underbrace{1 \cdot 1 \cdots 1}_n = \prod_{k=1}^n 1 = 1^n = 1;$$

$$\text{b) } \underbrace{0 \cdot 0 \cdots 0}_n = \prod_{k=1}^n 0 = 0^n = 0;$$

$$\text{d) } \underbrace{1 + 1 + \cdots + 1}_n = \sum_{k=1}^n 1 = n \cdot 1 = n.$$

Cvičení 7a.2 (poučné): Víme, že pro $a, b \in \mathbb{R}$ a $n \in \mathbb{N}_0$ platí $(ab)^n = a^n b^n$. U následujících pokusů o důkaz indukci určete, zda jsou správné, a pokud ne, tak najděte chybu.

Poznámka: Pro účely algebry bereme $0^0 = 1$.

$$\text{a) } (0) \ n = 0: (ab)^0 = 1 = 1 \cdot 1 = a^0 \cdot b^0.$$

$$(1) \text{ Dáno } n \geq 1: \text{IP: } (ab)^n = a^n b^n. \text{ Pak } (ab)^{n+1} = (ab)^n \cdot (ab) \stackrel{\text{IP}}{=} a^n b^n ab = a^{n+1} b^{n+1}.$$

$$\text{b) } (0) \ n = 0: (ab)^0 = 1 = 1 \cdot 1 = a^0 \cdot b^0.$$

$$(1) \text{ Předpokládejme, že } (ab)^n = a^n b^n. \text{ Pak } (ab)^{n+1} = (ab)^n \cdot (ab) \stackrel{\text{IP}}{=} a^n b^n ab = a^{n+1} b^{n+1}.$$

$$\text{c) } (0) \ n = 0: (ab)^0 = 1 = 1 \cdot 1 = a^0 \cdot b^0.$$

$$(1) \text{ Pro zvolené } n \geq 0 \text{ předpokládejme } (ab)^n = a^n b^n. \text{ Pak } (ab)^{n+1} = (ab)^n \cdot (ab) \stackrel{\text{IP}}{=} a^n b^n ab = a^{n+1} b^{n+1}.$$

$$\text{d) } (0) \ n = 0: (ab)^0 = 1 = 1 \cdot 1 = a^0 \cdot b^0.$$

$$(1) \text{ Dáno } n \geq 0: \text{IP: } (ab)^n = a^n b^n. \text{ Pak}$$

$$\begin{array}{l} (ab)^{n+1} = a^{n+1} b^{n+1} \\ (ab)^n ab = a^n ab^n b \quad / \text{ IP} \\ a^n b^n ab = a^n ab^n b \\ 1 = 1 \end{array}$$

$$\text{e) } (0) \ n = 0: (ab)^0 = 1 = 1 \cdot 1 = a^0 \cdot b^0.$$

$$(1) \text{ Předpokládejme, že } (ab)^n = a^n b^n \text{ pro } n \geq 0. \text{ Pak } (ab)^{n+1} = (ab)^n \cdot (ab) \stackrel{\text{IP}}{=} a^n b^n ab = a^{n+1} b^{n+1}.$$

$$\text{f) } (0) \ n = 0: (ab)^0 = 1 = 1 \cdot 1 = a^0 \cdot b^0.$$

$$(1) \text{ Dáno } n \geq 0, \text{IP: } (ab)^n = a^n b^n. \text{ Pak } (ab)^{n+1} = \underbrace{(ab)(ab) \cdots (ab)}_{n+1} = \underbrace{a \cdot a \cdots a}_{n+1} \cdot \underbrace{b \cdot b \cdots b}_{n+1} = a^{n+1} b^{n+1}.$$

Cvičení 7a.3 (rutinní, zkouškové): Dokažte indukci, že následující vzorce platí pro všechna $n \in \mathbb{N}$:

$$\text{a) } \sum_{k=1}^n (2k) = 2 + 4 + 6 + \cdots + (2n) = n(n+1);$$

$$\text{b) } \sum_{k=1}^n k = 1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1);$$

$$\text{c) } \sum_{k=1}^n k^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1);$$

$$\text{d) } \sum_{k=0}^n 2^k = 2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1;$$

$$\text{e) } \sum_{k=0}^n 4 \cdot 5^k = 4 \cdot 5^0 + 4 \cdot 5^1 + 4 \cdot 5^2 + \cdots + 4 \cdot 5^n = 5^{n+1} - 1;$$

$$\text{f) } \sum_{k=1}^n (e^k - e^{k-1}) = (e^1 - e^0) + (e^2 - e^1) + \cdots + (e^n - e^{n-1}) = e^n - 1;$$

$$\text{g) } \sum_{k=1}^n \ln\left(\frac{k}{k+1}\right) = \sum_{k=1}^n (\ln(k) - \ln(k+1)) = (\ln(1) - \ln(2)) + (\ln(2) - \ln(3)) + \cdots + (\ln(n) - \ln(n+1)) = -\ln(n+1);$$

$$\text{h) } \sum_{k=1}^n \frac{1}{(2k-1) \cdot (2k+1)} = \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \cdots + \frac{1}{(2n-1) \cdot (2n+1)} = \frac{n}{2n+1};$$

$$\text{i) } \sum_{k=1}^n k \cdot k! = 1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1.$$

Cvičení 7a.4 (rutinní, zkouškové, *dobré): Dokažte indukci následující nerovnosti:

$$\text{a) } 3n + 1 \leq 2^n \text{ pro } n \geq 4;$$

$$\text{e) } \sum_{k=0}^n 3^k \leq 5^n \text{ pro } n \in \mathbb{N};$$

b) $n^2 \geq 3n + 5$ pro $n \geq 5$;

f) $\sum_{k=0}^n 3^k \geq 2^n$ pro $n \in \mathbb{N}$;

c)* $n^2 \leq 4^n$ pro $n \in \mathbb{N}$;

g) $1 + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!} \leq 2 - \frac{1}{n!}$ pro $n \in \mathbb{N}$;

d) $n! < n^n$ pro $n \geq 2$;

h) $1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$ pro $n \in \mathbb{N}$.

Cvičení 7a.5 (rutinní, zkouškové): Dokažte matematickou indukcí následující tvrzení pro $n \in \mathbb{N}_0$:

a) 4 dělí $7^n - 3^n$;

c) $2n^2 + 6n$ je násobkem 4;

b) $4^n - 1$ je násobkem 3;

d) 4 dělí $5^n + 3$.

Cvičení 7a.6 (rutinní): Najděte $f(1)$, $f(2)$, $f(3)$, $f(4)$ pro f definované indukci jako

a) (0) $f(1) = 1$, (1) $f(n+1) = f(n) + 2$ pro $n \in \mathbb{N}$;

b) (0) $f(0) = 1$, (1) $f(n+1) = 3f(n)$ pro $n \in \mathbb{N}$;

c) (0) $f(0) = 1$, (1) $f(n+1) = 3f(n)$ pro $n \in \mathbb{N}_0$;

d) (0) $f(2) = 3$, (1) $f(n+1) = 2f(n) - n$ pro $n \geq 2$;

e) (0) $f(0) = 1$, (1) $f(n+1) = 2^{f(n)}$ pro $n \in \mathbb{N}_0$;

f) (0) $f(0) = 1$, (1) $f(n+1) = f(n)^2 + f(n) + 1$ pro $n \in \mathbb{N}_0$.

Cvičení 7a.7 (poučné): U následujících definic funkce f rozhodněte, která je dobře a která je chybná.

a) (0) $f(1) = 13$, (1) $f(n+1) = f(n) \cdot n$ pro $n \geq 2$;

b) (0) $f(1) = 13$, (1) $f(n+1) = f(n) + n$ pro $n \geq 1$;

c) (0) $f(1) = 13$, (1) $f(n+1) = f(n) + 13$ pro $n \geq 0$.

Cvičení 7a.8 (rutinní, zkouškové): Uvažujte funkce definované induktivně následujícími vzorci. Pro každou z nich spočítejte několik hodnot a zkuste odhadnout, jakým vzorcem je $f(n)$ dáno. Pak dokažte, že je to správně.

a) (0) $f(0) = 0$, (1) $f(n+1) = 2f(n)$ pro $n \in \mathbb{N}_0$;

b) (0) $f(1) = 0$, (1) $f(n+1) = f(n) + 1$ pro $n \in \mathbb{N}$;

c) (0) $f(1) = 1$, (1) $f(n+1) = f(n) \cdot \frac{n}{n+1}$ pro $n \in \mathbb{N}$;

d) (0) $f(0) = 1$, (1) $f(n+1) = -f(n)$ pro $n \geq 0$.

Cvičení 7a.9 (rutinní, *dobré): Uvažujte funkci f definovanou induktivně takto:

$(0_D) f(1) = 0$,

$(1_D) f(n+1) = 3f(n) + n$ pro $n \geq 1$.

Dokažte následující odhady:

a) $f(n) \geq n$ pro $n \geq 3$;

b) $f(n) \leq n!$ pro $n \geq 3$;

c)* $f(n) \leq 5^n$ pro $n \geq 1$.

Budete muset nejprve spočítat $f(2)$ a $f(3)$.**Cvičení 7a.10** (poučné): Najděte chybu v následujícím „důkazu“, že pro všechna nenulová reálná a a pro všechna $n \in \mathbb{N}_0$ platí $a^n = 1$.

(0) Pro $n = 0$ evidentně platí $a^0 = 1$.

(1) Nechť $n \geq 0$, předpokládejme $a^n = 1$. Pak $a^{n+1} = \frac{a^n \cdot a^n}{a^{n-1}} = \frac{1 \cdot 1}{1} = 1$.

Cvičení 7a.11 (poučné): Pro každou z následujících rovností $V(n)$ dokažte, že pro všechna $n \in \mathbb{N}$ platí implikace $V(n) \implies V(n+1)$.

a) $a^n = 0$ pro všechna $a \in \mathbb{R}$;

b) $2 + 4 + 6 + \dots + 2n = n^2 + n - 13$;

c) $1 + 2 + 3 + \dots + n = \frac{1}{2}(n-1)(n+2)$.

Ovšem jsou to zjevně nepravdivá tvrzení.

Cvičení 7a.12 (rutinní, poučné): Uvažujme matici $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, kde $a, b \in \mathbb{R}$. Dokažte, že pak pro všechna $k \in \mathbb{N}$ platí $A^k = \begin{pmatrix} a^k & 0 \\ 0 & b^k \end{pmatrix}$.**Cvičení 7a.13** (rutinní, poučné): Nechť $a_k \in \mathbb{R}$ pro $k \in \mathbb{N}$, $c \in \mathbb{R}$. Dokažte, že pro $n \in \mathbb{N}$ platí následující:

a) $\sum_{k=1}^n (ca_k) = c \sum_{k=1}^n a_k$;

b) $\prod_{k=1}^n (ca_k) = c^n \prod_{k=1}^n a_k$.

Cvičení 7a.14 (rutinní, poučné): Dokažte, že pro $q \neq 1$ a $n \in \mathbb{N}_0$ platí $\sum_{k=0}^n q^k = 1 + q + q^2 + \dots + q^n = \frac{q^{n+1} - 1}{q - 1}$.**Cvičení 7a.15** (poučné): Pro reálná (i komplexní) čísla (a dokonce pro vektory) je důležitá známá „trojúhelníková nerovnost“ $|x + y| \leq |x| + |y|$. Dokažte její následující zobecnění:

Jestliže $x_1, \dots, x_n \in \mathbb{R}$, pak $\left| \sum_{k=1}^n x_k \right| \leq \sum_{k=1}^n |x_k|$.

Cvičení 7a.16 (rutinní, poučné): Nechť $n \in \mathbb{N}$. Dokažte matematickou indukcí na k , že když $a, u \in \mathbb{Z}$ splňují $a \equiv u \pmod{n}$, pak pro libovolné $k \in \mathbb{N}$ platí $a^k \equiv u^k \pmod{n}$ (viz fakt 2a.20).

Cvičení 7a.17 (poučné): Nechť $n_1, n_2, \dots, n_m \in \mathbb{N}$ jsou po dvou nesoudělná. Označme $n = n_1 \cdot n_2 \cdots n_m$. Dokažte matematickou indukcí na m , že jestliže $a, b \in \mathbb{Z}$ splňují $a \equiv b \pmod{n_i}$ pro všechna $i = 1, \dots, m$, pak $a \equiv b \pmod{n}$.

Viz lemma 2a.18, bude se hodit lemma 2a.17.

Další zajímavá pravidla se dokazují indukcí v kapitole o kongruenci (cvičení 2a.11), v kapitole o relacích (cvičení 4c.1 a 4c.7) a v kapitole o zobrazení (cvičení 8a.12 a 8a.13).

Cvičení 7a.18 (poučné): Dokažte tzv. Bernoulliho nerovnost: Jestliže $h > -1$, pak $(1+h)^n \geq 1+hn$ pro všechna $n \in \mathbb{N}_0$.

Cvičení 7a.19 (poučné, dobré): Nechť $a, b \in \mathbb{Z}$. Dokažte indukcí, že $(a-b)$ dělí $(a^n - b^n)$ pro všechna $n \in \mathbb{N}$. Nápoředa: Od výrazu $a^{n+1} - b^{n+1}$ odeberte a zase přidejte $a^n b$ a chytře vytkněte.

Cvičení 7a.20 (poučné): Zkuste dokázat indukcí, že pro $n \in \mathbb{N}$ platí $\sum_{k=1}^n \frac{1}{2^k} = \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} \leq 1$.

a) Použijte dekompozici $\sum_{k=1}^n \frac{1}{2^k} = \sum_{k=1}^n \frac{1}{2^k} + \frac{1}{2^{n+1}}$.

b) Použijte trikovou dekompozici $\sum_{k=1}^{n+1} \frac{1}{2^k} = \frac{1}{2} + \sum_{k=2}^{n+1} \frac{1}{2^k} = \frac{1}{2} + \frac{1}{2} \sum_{k=1}^n \frac{1}{2^k}$.

Lépe je to vidět ve formě $\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^{n+1}} = \frac{1}{2} + \frac{1}{2} \left(\frac{1}{2} + \cdots + \frac{1}{2^n} \right)$.

Cvičení 7a.21 (poučné, dobré): Pokusíme se sečíst všechna čísla typu $\frac{1}{k}$. Definujme

$$H(n) = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

Dokažte, že pro všechna $n \in \mathbb{N}$ platí následující:

a) $H(2^n) \leq 1 + n$;

b) $H(2^n) \geq 1 + \frac{n}{2}$.

To ukazuje, že pro n typu 2^k máme $H(n) \approx \log_2(n)$.

Nápoředa: $\frac{1}{2^{n+1}} \leq \frac{1}{2^n}, \frac{1}{2^{n+2}} \leq \frac{1}{2^n}, \dots, \frac{1}{2^{n+2^{n-1}}} \leq \frac{1}{2^n}, \frac{1}{2^{n+2^n}} = \frac{1}{2^{n+1}} \leq \frac{1}{2^n}$.

Také $\frac{1}{2^{n+1}} \geq \frac{1}{2^{n+1}}, \frac{1}{2^{n+2}} \geq \frac{1}{2^{n+1}}, \dots, \frac{1}{2^{n+2^{n-1}}} \geq \frac{1}{2^{n+1}}, \frac{1}{2^{n+2^n}} = \frac{1}{2^{n+1}}$.

Cvičení 7a.22 (poučné, dobré):

a) Uvažujme $V(n): \frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2n-1}{2n} < \frac{1}{\sqrt{3n}}$.

Ukažte, že $V(1)$ platí.

Ukažte, že standardní indukční důkaz $V(n) \implies V(n+1)$ nelze provést.

b) Uvažujme $W(n): \frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2n-1}{2n} < \frac{1}{\sqrt{3n+1}}$. Dokažte, že platí pro $n \geq 2$.

c) Pomocí $W(n)$ dokažte, že $V(n)$ platí pro všechna $n \in \mathbb{N}$.

Řešení:

7a.1: a) (0) $n = 1: 0 = 0$ platí. (1) Dáno $n \in \mathbb{N}$, IP: $\underbrace{0 + 0 + \cdots + 0}_n = 0$. Pak $\underbrace{0 + 0 + \cdots + 0}_{n+1} = \underbrace{0 + 0 + \cdots + 0}_n + 0 \stackrel{\text{IP}}{=} 0 + 0 = 0$.

$0 + 0 = 0$.

a) (0) $n = 1: 0 = 0$ platí. (1) Dáno $n \in \mathbb{N}$, IP: $\sum_{k=1}^n 0 = 0$. Pak $\sum_{k=1}^{n+1} 0 = \sum_{k=1}^n 0 + 0 \stackrel{\text{IP}}{=} 0 + 0 = 0$.

a) (0) $n = 1: 1 \cdot 0 = 0$ platí. (1) Dáno $n \in \mathbb{N}$, IP: $n \cdot 0 = 0$. Pak $(n+1) \cdot 0 = n \cdot 0 + 1 \cdot 0 \stackrel{\text{IP}}{=} 0 + 0 = 0$.

b) (0) $n = 1: 0 = 0$ platí. (1) Dáno $n \in \mathbb{N}$, IP: $\underbrace{0 \cdot 0 \cdots 0}_n = 0$. Pak $\underbrace{0 \cdot 0 \cdots 0}_{n+1} = \underbrace{0 \cdot 0 \cdots 0}_n \cdot 0 \stackrel{\text{IP}}{=} 0 \cdot 0 = 0$.

b) (0) $n = 1: 0 = 0$ platí. (1) Dáno $n \in \mathbb{N}$, IP: $\prod_{k=1}^n 0 = 0$. Pak $\prod_{k=1}^{n+1} 0 = \left(\prod_{k=1}^n 0 \right) \cdot 0 \stackrel{\text{IP}}{=} 0 \cdot 0 = 0$.

b) (0) $n = 1: 0^1 = 0$ platí. (1) Dáno $n \in \mathbb{N}$, IP: $0^n = 0$. Pak $0^{n+1} = 0^n \cdot 0 \stackrel{\text{IP}}{=} 0 \cdot 0 = 0$.

c) (0) $n = 1: 1 = 1$ platí. (1) Dáno $n \in \mathbb{N}$, IP: $\underbrace{1 \cdot 1 \cdots 1}_n = 1$. Pak $\underbrace{1 \cdot 1 \cdots 1}_{n+1} = \underbrace{1 \cdot 1 \cdots 1}_n \cdot 1 \stackrel{\text{IP}}{=} 1 \cdot 1 = 1$.

c) (0) $n = 1: 1 = 1$ platí. (1) Dáno $n \in \mathbb{N}$, IP: $\prod_{k=1}^n 1 = 1$. Pak $\prod_{k=1}^{n+1} 1 = \left(\prod_{k=1}^n 1 \right) \cdot 1 \stackrel{\text{IP}}{=} 1 \cdot 1 = 1$.

c) (0) $n = 1: 1^1 = 1$ platí. (1) Dáno $n \in \mathbb{N}$, IP: $1^n = 1$. Pak $1^{n+1} = 1^n \cdot 1 \stackrel{\text{IP}}{=} 1 \cdot 1 = 1$.

d) (0) $n = 1: 1 = 1$ platí. (1) Dáno $n \in \mathbb{N}$, IP: $\underbrace{1 + 1 + \dots + 1}_n = n$. Pak $\underbrace{1 + 1 + \dots + 1}_{n+1} = \underbrace{1 + 1 + \dots + 1}_n + 1 \stackrel{\text{IP}}{=} n + 1$.

d) (0) $n = 1: 1 = 1$ platí. (1) Dáno $n \in \mathbb{N}$, IP: $\sum_{k=1}^n 1 = n$. Pak $\sum_{k=1}^{n+1} 1 = \sum_{k=1}^n 1 + 1 \stackrel{\text{IP}}{=} n + 1$.

d) (0) $n = 1: 1 \cdot 1 = 1$ platí. (1) Dáno $n \in \mathbb{N}$, IP: $n \cdot 1 = n$. Pak $(n + 1) \cdot 1 = n \cdot 1 + 1 \cdot 1 \stackrel{\text{IP}}{=} n + 1$.

7a.2: a) Chybná návaznost kroků, (1) má být pro $n \geq 0$.

b) Chybí specifikace, pro jaká n se dokazuje (1).

c) korektní důkaz

d) Implikace (1) „dokázána“ zpětným chodem.

e) Předpoklad proveden pro všechna $n \in \mathbb{N}_0$, což není správně.

f) V důkazu případu $n + 1$ se nepoužil IP, nejde o důkaz indukci.

7a.3: a) (0) $n = 1: 2 = 1 \cdot 2$ OK. (1) $n \in \mathbb{N}$. IP: $2 + 4 + 6 + \dots + (2n) = n(n + 1)$. Pak $2 + 4 + 6 + \dots + (2n + 2) = [2 + 4 + 6 + \dots + (2n)] + (2n + 2) \stackrel{\text{IP}}{=} n(n + 1) + (2n + 2) = n^2 + 3n + 2 = (n + 1)(n + 2)$.

b) (0) $n = 1: 1 = \frac{1}{2} \cdot 2$, platí. (1) $n \in \mathbb{N}$, IP: $1 + 2 + 3 + \dots + n = \frac{1}{2}n(n + 1)$. Pak $1 + 2 + 3 + \dots + (n + 1) = [1 + 2 + 3 + \dots + n] + (n + 1) \stackrel{\text{IP}}{=} \frac{1}{2}n(n + 1) + (n + 1) = \frac{1}{2}(n^2 + 3n + 2) = \frac{1}{2}(n + 1)(n + 2)$.

c) (0) $n = 1: 1^2 = \frac{1}{6} \cdot 2 \cdot 3$, platí. (1) $n \in \mathbb{N}$, IP: $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{1}{6}n(n + 1)(2n + 1)$. Pak $1^2 + 2^2 + 3^2 + \dots + (n + 1)^2 = [1^2 + 2^2 + 3^2 + \dots + n^2] + (n + 1)^2 \stackrel{\text{IP}}{=} \frac{1}{6}n(n + 1)(2n + 1) + (n + 1)^2 = \frac{1}{6}(2n^3 + 9n^2 + 13n + 6) = \frac{1}{6}(n + 1)(n + 2)(2n + 3) = \frac{1}{6}(n + 1)((n + 1) + 1)(2(n + 1) + 1)$.

d) (0) $n = 1: 2^0 + 2^1 = 3 = 4 - 1 = 2^2 - 1$. (1) $n \in \mathbb{N}$, IP: $\sum_{k=0}^n 2^k = 2^{n+1} - 1$. Pak $\sum_{k=0}^{n+1} 2^k = \sum_{k=0}^n 2^k + 2^{n+1} \stackrel{\text{IP}}{=} 2^{n+1} - 1 + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1$.

e) (0) $n = 1: 4 \cdot 5^0 + 4 \cdot 5^1 = 24 = 5^2 - 1$. (1) $n \in \mathbb{N}$, IP: $\sum_{k=0}^n 4 \cdot 5^k = 5^{n+1} - 1$. Pak $\sum_{k=0}^{n+1} 4 \cdot 5^k = \sum_{k=0}^n 4 \cdot 5^k + 4 \cdot 5^{n+1} \stackrel{\text{IP}}{=} 5^{n+1} - 1 + 4 \cdot 5^{n+1} = 5 \cdot 5^{n+1} - 1 = 5^{n+2} - 1$.

f) (0) $n = 1: e^1 - e^0 = e^1 - 1$. (1) $n \in \mathbb{N}$, IP: $\sum_{k=1}^n (e^k - e^{k-1}) = e^n - 1$. Pak $\sum_{k=1}^{n+1} (e^k - e^{k-1}) = \sum_{k=1}^n (e^k - e^{k-1}) + (e^{n+1} - e^n) \stackrel{\text{IP}}{=} e^n - 1 + e^{n+1} - e^n = e^{n+1} - 1$.

g) (0) $n = 1: \ln(1) - \ln(2) = 0 - \ln(2) = -\ln(2)$. (1) $n \in \mathbb{N}$, IP: $\sum_{k=1}^n (\ln(k) - \ln(k + 1)) = -\ln(n + 1)$. Pak

$\sum_{k=1}^{n+1} (\ln(k) - \ln(k + 1)) = \sum_{k=1}^n (\ln(k) - \ln(k + 1)) + (\ln(n + 1) - \ln(n + 2)) \stackrel{\text{IP}}{=} -\ln(n + 1) + \ln(n + 1) - \ln(n + 2) = -\ln(n + 2)$.

h) (0) $n = 1: \frac{1}{3} = \frac{1}{3}$. (1) $n \in \mathbb{N}$, IP: $\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \dots + \frac{1}{(2n-1) \cdot (2n+1)} = \frac{n}{2n+1}$. Pak $\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \dots + \frac{1}{(2n+1) \cdot (2n+3)} = [\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \dots + \frac{1}{(2n-1) \cdot (2n+1)}] + \frac{1}{(2n+1) \cdot (2n+3)} \stackrel{\text{IP}}{=} \frac{n}{2n+1} + \frac{1}{(2n+1) \cdot (2n+3)} = \frac{2n^2 + 3n + 1}{(2n+1)(2n+3)} = \frac{n+1}{2n+3} = \frac{n+1}{2(n+1)+1}$.

i) (0) $n = 1: 1 \cdot 1 = 2 - 1$. (1) $n \in \mathbb{N}$, IP: $1 \cdot 1! + 2 \cdot 2! + \dots + n \cdot n! = (n + 1)! - 1$. Pak $1 \cdot 1! + 2 \cdot 2! + \dots + n \cdot n! + (n + 1) \cdot (n + 1)! = [1 \cdot 1! + 2 \cdot 2! + \dots + n \cdot n!] + (n + 1) \cdot (n + 1)! \stackrel{\text{IP}}{=} [(n + 1)! - 1] + (n + 1) \cdot (n + 1)! = (n + 1)! + (n + 1) \cdot (n + 1)! - 1 = (n + 2)(n + 1)! - 1 = (n + 2)! - 1$.

7a.4: a) (0) $n = 4: 3 \cdot 4 + 1 = 13 \leq 16 = 2^4$. (1) $n \geq 4$, IP: $3n + 1 < 2^n$. Pak $3(n + 1) + 1 = (3n + 1) + 3 \stackrel{\text{IP}}{\leq} 2^n + 3 \leq 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$ díky $3 \leq 2^n$ pro $n \geq 4$.

(b) (0) $n = 5: 5^2 = 25 \geq 20 = 3 \cdot 5 + 5$. (1) $n \geq 5$, IP: $n^2 \geq 3n + 5$. Pak $(n + 1)^2 = n^2 + 2n + 1 \stackrel{\text{IP}}{\geq} (3n + 5) + 2n + 1 = 3n + 3 - 3 + 5 + 2n + 1 = 3(n + 1) + 5 + (2n - 2) \geq 3(n + 1) + 5$ díky $2n - 2 \geq 0$ pro $n \geq 5$.

c) (0) $n = 1: 1^2 = 1 \leq 4 = 4^1$. (1) $n \in \mathbb{N}$, IP: $n^2 \leq 4^n$. Pak $(n + 1)^2 = n^2 + 2n + 1 \stackrel{\text{IP}}{\leq} 4^n + 2n + 1 \leq 4^n + 2 \cdot 4^n + 4^n = 4 \cdot 4^n = 4^{n+1}$ díky $n \leq 4^n$ a $1 \leq 4^n$ pro $n \in \mathbb{N}$, to první bychom museli dokázat indukci.

d) (0) $n = 2: 2! = 2 < 4 = 2^2$. (1) $n \geq 2$, IP: $n! < n^n$. Pak $(n + 1)! = (n + 1)n! \stackrel{\text{IP}}{<} (n + 1)n^n < (n + 1)(n + 1)^n = (n + 1)^{n+1}$.

e) (0) $n = 1: 3^0 + 3^1 = 4 \leq 5 = 5^1$. (1) $n \in \mathbb{N}$, IP: $\sum_{k=0}^n 3^k \leq 5^n$. Pak $\sum_{k=0}^{n+1} 3^k = \sum_{k=0}^n 3^k + 3^{n+1} \stackrel{\text{IP}}{\leq} 5^n + 3^{n+1} = 5^n + 3 \cdot 3^n \leq 5^n + 3 \cdot 5^n = 4 \cdot 5^n \leq 5 \cdot 5^n = 5^{n+1}$.

f) (0) $n = 1: 3^0 + 3^1 = 4 \geq 2 = 2^1$. (1) $n \in \mathbb{N}$, IP: $\sum_{k=0}^n 3^k \geq 2^n$. Pak $\sum_{k=0}^{n+1} 3^k = \sum_{k=0}^n 3^k + 3^{n+1} \stackrel{\text{IP}}{\geq} 2^n + 3^n \geq 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$.

g) (0) $n = 1: 1 \leq 2 - 1$. (1) $n \in \mathbb{N}$, IP: $1 + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!} \leq 2 - \frac{1}{n!}$. Pak $1 + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{(n+1)!} = [1 + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!}] + \frac{1}{(n+1)!} \stackrel{\text{IP}}{\leq} [2 - \frac{1}{n!}] + \frac{1}{(n+1)!} = 2 - \frac{(n+1)-1}{(n+1)!} = 2 - \frac{n}{(n+1)!} \leq 2 - \frac{1}{(n+1)!}$.

h) (0) $n = 1: 1 \leq 2 - 1$. (1) $n \in \mathbb{N}$, IP: $1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$. Pak $1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{(n+1)^2} = [1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2}] + \frac{1}{(n+1)^2} \stackrel{\text{IP}}{\leq} [2 - \frac{1}{n}] + \frac{1}{(n+1)^2} = 2 - \frac{(n+1)^2 - n}{n(n+1)^2} = 2 - \frac{n^2 + n + 1}{n(n+1)^2} \leq 2 - \frac{n^2 + n}{n(n+1)^2} = 2 - \frac{1}{n+1}$.

7a.5: a) (0) $n = 0: 7^0 - 3^0 = 1 - 1 = 0 = 4 \cdot 0$, kde $k = 0 \in \mathbb{Z}$. (1) $n \geq 0$, IP: $7^n - 3^n = 4k$ pro $k \in \mathbb{Z}$. Pak $7^{n+1} - 3^{n+1} = 7 \cdot 7^n - 3 \cdot 3^n = (4+3) \cdot 7^n - 3 \cdot 3^n = 4 \cdot 7^n + 3(7^n - 3^n) \stackrel{\text{IP}}{=} 4 \cdot 7^n + 3 \cdot 4k = 4(7^n + 3k)$, kde $7^n + 3k \in \mathbb{Z}$.

b) (0) $n = 0: 4^0 - 1 = 1 - 1 = 0 = 3 \cdot 0$, kde $k = 0 \in \mathbb{Z}$. (1) $n \geq 0$, IP: $4^n - 1 = 3k$ pro $k \in \mathbb{Z}$. Pak $4^{n+1} - 1 = 4 \cdot 4^n - 1 = 4(4^n - 1 + 1) - 1 = 4(4^n - 1) + 3 \stackrel{\text{IP}}{=} 4 \cdot 3k + 3 = 3(4k + 1)$, kde $4k + 1 \in \mathbb{Z}$.

c) (0) $n = 0: 2 \cdot 0^2 + 6 \cdot 0 = 0 = 4 \cdot 0$, kde $k = 0 \in \mathbb{Z}$. (1) $n \geq 0$, IP: $2n^2 + 6n = 4k$ pro $k \in \mathbb{Z}$. Pak $2(n+1)^2 + 6(n+1) = 2n^2 + 4n + 2 + 6n + 6 = (2n^2 + 6n) + (4n + 8) \stackrel{\text{IP}}{=} 4k + 4(n+2) = 4(k+n+2)$, kde $k+n+2 \in \mathbb{Z}$.

d) (0) $n = 0: 5^0 + 3 = 4 = 4 \cdot 1$, kde $k = 1 \in \mathbb{Z}$. (1) $n \geq 0$, IP: $5^n + 3 = 4k$ pro $k \in \mathbb{Z}$. Pak $5^{n+1} + 3 = 5 \cdot 5^n + 3 = 5(5^n + 3 - 3) + 3 = 5(5^n - 1) - 12 \stackrel{\text{IP}}{=} 5 \cdot 4k - 12 = 4(5k - 3)$, kde $5k - 3 \in \mathbb{Z}$.

7a.6: a) $f(1) = 1, f(2) = f(1) + 2 = 3, f(3) = f(2) + 2 = 5, f(4) = 7$. b) Nelze. Rádi bychom udělali $f(1) = 3f(0)$, ale ve vzorci $f(0+1) = 3f(0)$ je $n = 0$ a tento vzorec je v definici až pro $n \geq 1$. c) $f(1) = 3f(0) = 3, f(2) = 3f(1) = 9, f(3) = 27, f(4) = 81$. d) $f(1)$ neexistuje, $f(2) = 3, f(3) = 2f(2) - 2 = 4, f(4) = 2f(3) - 3 = 5$. e) $f(1) = 2^{f(0)} = 2, f(2) = 2^{f(1)} = 4, f(3) = 16, f(4) = 2^{16} (= 65536)$. f) $f(1) = f(0)^2 + f(0) + 1 = 3, f(2) = f(1)^2 + f(1) + 1 = 13, f(3) = 183, f(4) = 183^2 + 183 + 1 (= 33673)$.

7a.7: a) Chybná, Buď musí (1) platit od $n \geq 1$, nebo je třeba v (0) zadat $f(2)$. b) korektní. c) Pravidlo (1) pro $n = 0$ je zbytečné a ani nelze použít, protože chybí vstupní data. Funkce sice vznikne, ale nesprávnou definicí.

7a.8: a) $f(n) = 0$. (0) $n = 0$ funguje. (1) $n \in \mathbb{N}_0$, IP: $f(n) = 0$. Pak $f(n+1) = 2f(n) \stackrel{\text{IP}}{=} 2 \cdot 0 = 0$.

b) $f(n) = n - 1$. (0) $n = 1$ funguje. (1) $n \in \mathbb{N}$, IP: $f(n) = n - 1$. Pak $f(n+1) = f(n) + 1 \stackrel{\text{IP}}{=} n - 1 + 1 = (n+1) - 1$.

c) $f(n) = \frac{1}{n}$. (0) $n = 1$ funguje. (1) $n \in \mathbb{N}$, IP: $f(n) = \frac{1}{n}$. Pak $f(n+1) = f(n) \cdot \frac{n}{n+1} \stackrel{\text{IP}}{=} \frac{1}{n} \cdot \frac{n}{n+1} = \frac{1}{n+1}$.

d) $f(n) = (-1)^n$. (0) $n = 0$ funguje. (1) $n \in \mathbb{N}_0$, IP: $f(n) = (-1)^n$. Pak $f(n+1) = -f(n) \stackrel{\text{IP}}{=} -(-1)^n = (-1) \cdot (-1)^n = (-1)^{n+1}$.

7a.9: $f(2) = 3f(1) + 1 = 1, f(3) = 3f(2) + 2 = 5$.

a) (0) $f(3) = 5 \geq 3$. (1) $n \geq 3$, IP: $f(n) \geq n$. Pak $f(n+1) = 3f(n) + n \stackrel{\text{IP}}{\geq} 3n + n \geq 1 + n = n + 1$ díky $3n \geq 1$ pro $n \geq 3$.

b) (0) $f(3) = 5 \leq 6 = 3!$. (1) $n \geq 3$, IP: $f(n) \leq n!$. Pak $f(n+1) = 3f(n) + n \stackrel{\text{IP}}{\leq} 3n! + n \leq 3n! + n! = 4n! \leq (n+1)n! = (n+1)!$ díky $4 \leq n+1$ pro $n \geq 3$.

Poznámka: Nerovnost $3n! + n \leq (n+1)!$ platí také pro $n = 1, 2$, ale indukční krok by se dokazoval obtížněji.

c) (0) $f(1) = 0 \leq 5 = 5^1$. (1) $n \in \mathbb{N}$, IP: $f(n) \leq 5^n$. Pak $f(n+1) = 3f(n) + n \stackrel{\text{IP}}{\leq} 3 \cdot 5^n + n \leq 3 \cdot 5^n + 5^n = 4 \cdot 5^n \leq 5 \cdot 5^n = 5^{n+1}$ díky $n \leq 5^n$ pro $n \in \mathbb{N}$, to by se muselo dokázat (také indukci).

7a.10: V indukčním kroku je použito $a^{n-1} = 1$, což ale nemusí platit, indukční předpoklad dává jen $a^n = 1$.

7a.11: a) $n \in \mathbb{N}$, IP: $a^n = 0$ pro všechna $a \in \mathbb{R}$. Pak pro $a \in \mathbb{R}$ máme $a^{n+1} = a^n \cdot a \stackrel{\text{IP}}{=} 0 \cdot a = 0$.

b) $n \in \mathbb{N}$, IP: $2 + 4 + 6 + \dots + 2n = n^2 + n - 13$. Pak $2 + 4 + 6 + \dots + 2(n+1) = [2 + 4 + 6 + \dots + 2n] + (2n+2) \stackrel{\text{IP}}{=} [n^2 + n - 13] + 2n + 2 = (n^2 + 2n + 1) + (n+1) - 13 = (n+1)^2 + (n+1) - 13$.

c) $n \in \mathbb{N}$, IP: $1 + 2 + 3 + \dots + n = \frac{1}{2}(n-1)(n+2)$. Pak $1 + 2 + 3 + \dots + (n+1) = [1 + 2 + 3 + \dots + n] + (n+1) \stackrel{\text{IP}}{=} \frac{1}{2}(n-1)(n+2) + (n+1) = \frac{1}{2}(n^2 + 3n) = \frac{1}{2}n(n+3)$.

7a.12: (0) Pro $n = 1$ platí. (1) $n \in \mathbb{N}$, IP: $A^n = \begin{pmatrix} a^n & 0 \\ 0 & b^n \end{pmatrix}$. Pak $A^{n+1} = A^n \cdot A \stackrel{\text{IP}}{=} \begin{pmatrix} a^n & 0 \\ 0 & b^n \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a^{n+1} & 0 \\ 0 & b^{n+1} \end{pmatrix}$.

7a.13: a) (0) $n = 1: \sum_{k=1}^1 (ca_k) = ca_1 = c \sum_{k=1}^1 a_k$. (1) $n \in \mathbb{N}$, IP: $\sum_{k=1}^n (ca_k) = c \sum_{k=1}^n a_k$. Pak $\sum_{k=1}^{n+1} (ca_k) = \sum_{k=1}^n (ca_k) + (ca_{n+1}) \stackrel{\text{IP}}{=} c \sum_{k=1}^n a_k + c(a_{n+1}) = c(\sum_{k=1}^n a_k + a_{n+1}) = c \sum_{k=1}^{n+1} a_k$.

b) (0) $n = 1: \prod_{k=1}^1 (ca_k) = ca_1 = c \prod_{k=1}^1 a_k$. (1) $n \in \mathbb{N}$, IP: $\prod_{k=1}^n (ca_k) = c^n \prod_{k=1}^n a_k$. Pak $\prod_{k=1}^{n+1} (ca_k) = (\prod_{k=1}^n (ca_k)) \cdot (ca_{n+1}) \stackrel{\text{IP}}{=} c^n \prod_{k=1}^n a_k \cdot ca_{n+1} = c^{n+1} \prod_{k=1}^{n+1} a_k$.

$$c^n \left(\prod_{k=1}^n a_k \right) \cdot c \cdot a_{n+1} = c^{n+1} \left(\prod_{k=1}^n a_k \right) \cdot a_{n+1} = c^{n+1} \prod_{k=1}^{n+1} a_k.$$

7a.14: (0) $n = 0$: $1 = \frac{q^1-1}{q-1}$. (1) $n \geq 0$, IP: $\sum_{k=0}^n q^k = \frac{q^{n+1}-1}{q-1}$. Pak $\sum_{k=0}^{n+1} q^k = \sum_{k=0}^n q^k + q^{n+1} \stackrel{\text{IP}}{=} \frac{q^{n+1}-1}{q-1} + q^{n+1} = \frac{q^{n+1}-1}{q-1} + \frac{q^{n+2}-q^{n+1}}{q-1} = \frac{q^{n+2}-1}{q-1}$.

7a.15: (0) $n = 1$: $|x_1| = |x_1|$ platí. (1) $n \in \mathbb{N}$, IP: $\left| \sum_{k=1}^n x_k \right| \leq \sum_{k=1}^n |x_k|$. Pak $\left| \sum_{k=1}^{n+1} x_k \right| = \left| x_{n+1} + \sum_{k=1}^n x_k \right| \leq |x_{n+1}| + \left| \sum_{k=1}^n x_k \right| \stackrel{\text{IP}}{\leq} |x_{n+1}| + \sum_{k=1}^n |x_k| = \sum_{k=1}^{n+1} |x_k|$.

7a.16: (0) $k = 1$ jasné. (1) Necht' $k \in \mathbb{N}$. IP: $a^k \equiv u^k \pmod{n}$. Také $a \equiv u$, proto dle Věty 2a.7 (iii) platí $a^k \cdot a \equiv u^k \cdot u \pmod{n}$ neboli $a^{k+1} \equiv u^{k+1} \pmod{n}$.

7a.17: (0) $m = 1$ evidentně platí.

(1) Předpokládejme platnost pro m . Mějme n_1, \dots, n_m, n_{m+1} po dvou nesoudělná a a, b dle předpokladu. Protože $a \equiv b \pmod{n_1}, \dots, a \equiv b \pmod{n_m}$, musí podle indukčního předpokladu platit $a \equiv b \pmod{n'}$, kde $n' = n_1 \cdot n_2 \cdot \dots \cdot n_m$. Také $a \equiv b \pmod{n_{m+1}}$, proto podle lemma 2a.17 platí $a \equiv b \pmod{n'n_{m+1}}$, ale $n'n_{m+1} = n_1 \cdot n_2 \cdot \dots \cdot n_m \cdot n_{m+1}$, přesně jak jsme potřebovali.

7a.18: (0) $n = 0$: $(1+h)^0 \geq 1+0$ platí.

(1) $n \in \mathbb{N}_0$, IP: pro každé $h > -1$ platí $(1+h)^n \geq 1+hn$. Pak pro $h > -1$ platí $(1+h)^{n+1} = (1+h)(1+h)^n \stackrel{\text{IP}}{\geq} (1+h)(1+hn) = 1+h(n+1)+h^2 \geq 1+h(n+1)$.

7a.19: (0) $n = 1$: $(a-b)$ dělí $a^1 - b^1 = a - b$. (1) $n \in \mathbb{N}$, IP: $a^n - b^n = (a-b)k$, kde $k \in \mathbb{Z}$. Pak $a^{n+1} - b^{n+1} = a^{n+1} - a^n b + a^n b - b^{n+1} = a^n(a-b) + b(a^n - b^n) \stackrel{\text{IP}}{=} a^n(a-b) + b(a-b)k = (a-b)(a^n + bk)$, kde $a^n + bk \in \mathbb{Z}$.

7a.20: (0) $n = 1$: $\frac{1}{2} \leq 1$ platí.

a) Dáno $n \geq 1$, IP: $\sum_{k=1}^n \frac{1}{2^k} \leq 1$. Pak $\sum_{k=1}^n \frac{1}{2^k} = \sum_{k=1}^n \frac{1}{2^k} + \frac{1}{2^{n+1}} \stackrel{\text{IP}}{\leq} 1 + \frac{1}{2^{n+1}}$ konec, nelze pokračovat $1 + \frac{1}{2^{n+1}} \leq 1$.

b) Dáno $n \geq 1$, IP: $\sum_{k=1}^n \frac{1}{2^k} \leq 1$. Pak $\sum_{k=1}^{n+1} \frac{1}{2^k} = \frac{1}{2} + \frac{1}{2} \sum_{k=1}^n \frac{1}{2^k} \stackrel{\text{IP}}{\leq} \frac{1}{2} + \frac{1}{2} \cdot 1 = 1$. Povedlo se.

7a.21: a) (0) $n = 1$: $1 + \frac{1}{2} \leq 2 = 1 + 1$, platí.

(1) $n \in \mathbb{N}$, IP: $H(2^n) \leq 1+n$. Pak $H(2^{n+1}) = 1 + \frac{1}{2} + \dots + \frac{1}{2^{n+1}} = \left[1 + \frac{1}{2} + \dots + \frac{1}{2^n} \right] + \frac{1}{2^{n+1}} + \frac{1}{2^{n+2}} + \dots + \frac{1}{2^{n+1}} \stackrel{\text{IP}}{\leq} 1 + n + \frac{1}{2^n} + \frac{1}{2^n} + \dots + \frac{1}{2^n} = 1 + n + 2^n \frac{1}{2^n} = 1 + (n+1)$, neboť zlomků od $\frac{1}{2^{n+1}}$ po $\frac{1}{2^{n+1}} = \frac{1}{2 \cdot 2^n} = \frac{1}{2^{n+2}}$ je přesně 2^n .

b) (0) $n = 1$: $H(2) \geq 1 + \frac{1}{2}$ znamená $1 + \frac{1}{2} \geq 1 + \frac{1}{2}$, platí.

(1) $n \in \mathbb{N}$, IP: $H(2^n) \geq 1 + \frac{n}{2}$. Pak $H(2^{n+1}) = 1 + \frac{1}{2} + \dots + \frac{1}{2^{n+1}} = \left[1 + \frac{1}{2} + \dots + \frac{1}{2^n} \right] + \frac{1}{2^{n+1}} + \frac{1}{2^{n+2}} + \dots + \frac{1}{2^{n+1}} \stackrel{\text{IP}}{\geq} 1 + \frac{n}{2} + \frac{1}{2^{n+1}} + \frac{1}{2^{n+1}} + \dots + \frac{1}{2^{n+1}} = 1 + \frac{n}{2} + 2^n \cdot \frac{1}{2^{n+1}} = 1 + \frac{n+1}{2}$.

7a.22: a) $V(1)$: $\frac{1}{2} < \frac{1}{\sqrt{3}}$ platí.

Zkusíme dokázat indukční krok: Předpoklad $\frac{1}{2} \cdot \frac{3}{4} \dots \frac{2n-1}{2n} < \frac{1}{\sqrt{3n}}$. Pak

$$\frac{1}{2} \cdot \frac{3}{4} \dots \frac{2n+1}{2n+2} = \frac{1}{2} \cdot \frac{3}{4} \dots \frac{2n-1}{2n} \cdot \frac{2n+1}{2n+2} < \frac{1}{\sqrt{3n}} \cdot \frac{2n+1}{2n+2}. \text{ Chceme, aby platilo } \frac{1}{\sqrt{3n}} \cdot \frac{2n+1}{2n+2} \leq \frac{1}{\sqrt{3(n+1)}} \text{ neboli}$$

$(2n+1)\sqrt{3(n+1)} \leq (2n+2)\sqrt{3n}$, odtud umocněním $n+1 \leq 0$. Toto neplatí nikdy, a protože kroky byly ekvivalentní, nemohla platit ani výchozí nerovnost. Indukční krok se tedy dokázat nepovede.

b) (0) $W(2)$: $\frac{1}{2} \cdot \frac{3}{4} < \frac{1}{\sqrt{7}}$ platí.

Předpokládejme $\frac{1}{2} \cdot \frac{3}{4} \dots \frac{2n-1}{2n} < \frac{1}{\sqrt{3n+1}}$. Pak $\frac{1}{2} \cdot \frac{3}{4} \dots \frac{2n+1}{2n+2} = \frac{1}{2} \cdot \frac{3}{4} \dots \frac{2n-1}{2n} \cdot \frac{2n+1}{2n+2} < \frac{1}{\sqrt{3n+1}} \cdot \frac{2n+1}{2n+2}$. Chceme, aby platilo $\frac{1}{\sqrt{3n+1}} \cdot \frac{2n+1}{2n+2} \leq \frac{1}{\sqrt{3(n+1)+1}}$.

Zkusíme postup od konce: přepíšeme nerovnost na $(2n+1)\sqrt{3n+4} < (2n+2)\sqrt{3n+1}$, odtud umocněním a po úpravě $0 \leq n$. To platí, neboť zde máme $n \geq 2$. Všechny kroky byly ekvivalentní včetně umocnění, protože se umocňovala kladná čísla. Postup lze proto obrátit a z pravdivého faktu $0 \leq n$ lze korektně dojít k žádané nerovnosti, pomocí ní dokončíme důkaz indukčního kroku:

$$\frac{1}{2} \cdot \frac{3}{4} \dots \frac{2n+1}{2n+2} < \dots < \frac{1}{\sqrt{3n+1}} \cdot \frac{2n+1}{2n+2} \leq \frac{1}{\sqrt{3(n+1)+1}}.$$

c) $V(1)$ už bylo ověřeno v a). Pokud $n \geq 2$, pak pomocí $W(n)$ máme $\frac{1}{2} \cdot \frac{3}{4} \dots \frac{2n-1}{2n} < \frac{1}{\sqrt{3n+1}} < \frac{1}{\sqrt{3n}}$.

7b. Silná indukce

Začneme inspirativním příkladem.

Příklad 7b.a: Dokážeme indukcí, že každé $n \in \mathbb{N}$ lze vyjádřit jako součet mocnin dvojky.

(0) $n = 1$: Platí $1 = 2^0$.

(1) Dáno $n \in \mathbb{N}$, předpokládejme, že existují $N \in \mathbb{N}$ a $m_k \in \mathbb{N}_0$, $k = 1, \dots, N$ takové, že $n = \sum_{k=1}^N 2^{m_k}$.

Uvažujme číslo $n + 1$. Podle indukčního předpokladu $n = \sum_{k=1}^N 2^{m_k}$ pro nějaká $m_k \in \mathbb{N}_0$, $k = 1, \dots, N$. Proto

$$n + 1 = \sum_{k=1}^N 2^{m_k} + 1 = \sum_{k=1}^N 2^{m_k} + 2^0.$$

□

To bylo snadné, ovšem pro binární rozklad čísla potřebujeme, aby ty mocniny dvojky byly různé. Náš postup to nezaručuje. Například pro $n + 1 = 14$ se odvoláme na indukční předpoklad $13 = 1 + 4 + 8 = 2^0 + 2^2 + 2^3$ a dojdeme k závěru, že $14 = 13 + 1 = 2^0 + 2^2 + 2^3 + 2^0$, kde se ovšem 2^0 opakuje dvakrát.

Abychom tomu zabránili, nebudeme z $n + 1$ odebírat jedničku neboli nejmenší mocninu dvojky, která se do $n + 1$ vleze, ale naopak tu největší. Vylepšený důkaz tedy bude v klíčové fázi fungovat takto: Najdeme největší $m \in \mathbb{N}_0$ takové, že $2^m \leq n + 1$, a přejdeme k číslu $n + 1 - 2^m$. Na něj bychom rádi aplikovali indukční předpoklad, ale máme smůlu. Číslo $n + 1 - 2^m$ totiž nemusí být rovno n , o kterém indukční předpoklad něco říká, popravdě řečeno typicky bude $n + 1 - 2^m$ mnohem menší než n . Například pro $n = 13$ bychom identifikovali $m = 3$, protože větší mocninu dvojky než 2^3 v čísle $13 + 1 = 14$ nenajdeme, a přešli bychom rekurzí k číslu $13 + 1 - 2^3 = 6$. O tom nám IP nic neříká, ten umí rozložit jen třináctku.

△

Narazili jsme na situaci, kdy chceme vyřešit případ $n + 1$ rekurzivně pomocí předchozích znalostí, ale ukázalo se, že nám nestačí umět řešit bezprostředního předchůdce n , ale potřebovali bychom znát víc o minulosti. Existují dva přístupy. Flexibilnější, teoreticky lepší, ale pro začátečníka náročnější je vytvořit uměle vlastnost, která zaznamená pro dané n informaci o celé minulosti od n_0 až po n .

Příklad 7b.b (návrat k 7b.a): Dokážeme indukcí, že každé $n \in \mathbb{N}$ lze vyjádřit jako součet mocnin dvojky, které se neopakují, tedy pro každé $n \in \mathbb{N}$ existují navzájem různá čísla $m_k \in \mathbb{N}_0$, kde $k = 1, \dots, N$ pro nějaké $N \in \mathbb{N}$, splňující $n = \sum_{k=1}^N 2^{m_k}$.

Jak jsme viděli, dokázat tuto vlastnost přímo je problematické. Proto si namísto formálního „ $V(n)$: n lze vhodně vyjádřit“ zavedeme silnější vlastnost, která zahrnuje informace o minulosti.

Uvažujme tedy vlastnost $W(n)$: Každé přirozené číslo od 1 po n včetně lze vyjádřit jako součet různých mocnin dvojky.

Pokud dokážeme platnost vlastnosti $W(n)$ pro všechna n , pak tím také dokážeme naše tvrzení.

(0) $n = 1$: Platí $1 = 2^0$, tedy všechna čísla mezi 1 až 1 lze vyjádřit jako součet různých mocnin dvojky.

(1) Dáno $n \in \mathbb{N}$, předpokládejme platnost $W(n)$, tedy že všechna přirozená čísla mezi 1 a n včetně lze vyjádřit jako součet různých mocnin dvojky. Ukážeme, že platí $W(n + 1)$.

Vezměme tedy přirozené číslo x mezi 1 a $n + 1$ včetně. Pokud platí $x \leq n$, pak přímo na toto x aplikujeme IP a dostaneme potřebné vyjádření. Zbývá vyřešit případ $x = n + 1$.

Nechť m je největší číslo z \mathbb{N}_0 takové, že $2^m \leq n + 1$. Toto číslo existuje, protože díky $2^0 = 1 \leq n + 1$ vybíráme z neprázdné množiny, která je omezená shora, neboť nerovnost $2^m \leq n + 1$ vede na $m \leq \log_2(n + 1)$.

Pokud $n + 1 = 2^m$, jsme hotovi. Pokud $2^m < n + 1$, pak je $n + 1 - 2^m > 0$, tedy je to přirozené číslo, a díky $2^m > 0$ splňuje $n + 1 - 2^m \leq n + 1 - 1 = n$. Můžeme tedy na něj aplikovat indukční předpoklad a dostáváme

$$n + 1 - 2^m = \sum_{k=1}^N 2^{m_k} \text{ s navzájem různými exponenty } m_k \in \mathbb{N}_0. \text{ Pak máme}$$

$$n + 1 = \sum_{k=1}^N 2^{m_k} + 2^m.$$

Zbývá ukázat, že nelze mít $m_k = m$. Sporem, předpokládejme, že jisté m_k splňuje $m_k = m$. Pak máme

$$n + 1 \geq 2^{m_k} + 2^m = 2^m + 2^m = 2 \cdot 2^m = 2^{m+1},$$

což je ve sporu s tím, že 2^m je nejvyšší mocnina dvojky, která nepřevyší $n + 1$.

Potvrdili jsme existenci vyjádření i pro $n + 1$, tedy máme ji pro všechna čísla 1 až $n + 1$ a $W(n + 1)$ platí.

□

△

Tento přístup má nicméně dvě nevýhody. Za prvé, zahrnuje významné plýtvání. V indukčním kroku rozšiřujeme platnost vlastnosti z množiny 1 až n na množinu 1 až $n+1$, ale ve skutečnosti to pro čísla 1 až n už víme, stačí jen přidat $n+1$. Bylo by pěkné si ověřování 1 až n ušetřit. Ještě lepší by bylo ušetřit náhradní vlastnost W a pracovat přímo s V . Vyplatí se proto zavést nový indukční princip.

7b.1. Silný princip matematické indukce.

Nechť $n_0 \in \mathbb{Z}$, nechť $V(n)$ je vlastnost celých čísel, která má smysl pro $n \geq n_0$.

Předpokládejme, že:

(0) platí $V(n_0)$.

(1) Pro každé $n \in \mathbb{Z}$, $n \geq n_0$ je pravdivá následující implikace:

Je-li $V(k)$ platí pro všechna $k = n_0, n_0 + 1, \dots, n$, pak platí také $V(n+1)$.

Potom $V(n)$ platí pro všechna $n \in \mathbb{Z}$, $n \geq n_0$.

Tomuto principu se také říká **úplná indukce**, anglický název je **Strong principle of mathematical induction**.

Vrátíme se k binárnímu rozkladu. Abychom jen nemodifikovali předchozí důkaz, použijeme jiný mechanismus přechodu k minulosti.

! Příklad 7b.c (návrat k 7b.a): Dokážeme indukcí, že pro každé $n \in \mathbb{N}$ existují navzájem různá čísla $m_k \in \mathbb{N}_0$, kde $k = 1, \dots, N$ pro nějaké $N \in \mathbb{N}$, splňující $n = \sum_{k=1}^N 2^{m_k}$.

Použijeme silnou indukci.

(0) $n = 1$: Platí $1 = 2^0$.

(1) Dáno $n \in \mathbb{N}$, předpokládejme, že všechna přirozená čísla mezi 1 až n včetně lze vyjádřit jako součet různých mocnin dvojky. Ukážeme, že to platí i pro $n+1$,

Případ 1: $n+1$ sudé. Protože $n+1 \geq 2$, je celé číslo $\frac{1}{2}(n+1)$ menší než $n+1$ a alespoň 1, tedy patří mezi čísla pokrytá indukčním předpokladem. Podle IP existuje rozklad $\frac{1}{2}(n+1) = \sum_{k=1}^N 2^{m_k}$ pro nějaká navzájem různá $m_k \in \mathbb{N}_0$. Pak

$$n+1 = 2 \sum_{k=1}^N 2^{m_k} = \sum_{k=1}^N 2^{m_k+1},$$

kde $m_k + 1 \in \mathbb{N}_0$ jsou navzájem různá čísla.

Případ 2: $n+1$ liché. Pak je n sudé a díky $n \geq 1$ platí $n \geq 2$. Proto je celé číslo $\frac{1}{2}n$ mezi 1 až n včetně a podle IP máme $\frac{1}{2}n = \sum_{k=1}^N 2^{m_k}$ pro nějaká navzájem různá $m_k \in \mathbb{N}_0$. Pak

$$n+1 = 2 \sum_{k=1}^N 2^{m_k} + 1 = \sum_{k=1}^N 2^{m_k+1} + 2^0,$$

kde $m_k + 1 \in \mathbb{N}_0$ jsou navzájem různá čísla, která jsou také různá od $m_{N+1} = 0$.

□

Teto přístup k redukci vyžaduje dokazovat indukční krok dvakrát, ale to je jen technický problém tohoto příkladu, samotný formát silné indukce byl efektivní.

△

! Jak naše kroky potvrdí platnost pro všechna n ? Platnost $V(1)$ jsme přímo ověřili v kroku (0). Teď využijeme dokázanou implikaci (1) pro případ $n = 1$, máme tedy $V(1) \implies V(2)$. My už ale víme, že $V(1)$ platí, proto díky implikaci musí platit i $V(2)$. Teď přejdeme ke kroku (1) s volbou $n = 2$, tedy máme potvrzenou implikaci $[V(1) \wedge V(2)] \implies V(3)$. Ovšem platnost $V(1)$ a $V(2)$ už máme, proto díky této implikaci platí i $V(3)$. Takto postupujeme a dojdeme ke všem přirozeným číslům. Zatímco slabá indukce funguje jako jakýsi řetězec:

$$\xrightarrow{(0)} V(1) \xrightarrow{(1)}_{n=1} V(2) \xrightarrow{(1)}_{n=2} V(3) \xrightarrow{(1)}_{n=3} \dots$$

silná indukce je spíše jakoby pyramidální:

$$\begin{array}{ccccccc} \xrightarrow{(0)} V(1) & & V(1) \xrightarrow{(1)}_{n=1} V(2) & & \left. \begin{array}{l} V(1) \\ V(2) \end{array} \right] \xrightarrow{(1)}_{n=2} V(3) & & \left. \begin{array}{l} V(1) \\ V(2) \\ V(3) \end{array} \right] \xrightarrow{(1)}_{n=3} V(4) & \text{atd.} \end{array}$$

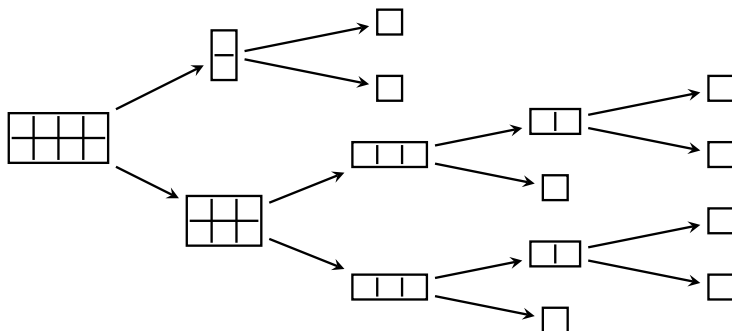
M Poznámka: Pro silnou indukci je třeba představu domin modifikovat. Jednotlivé očíslované kostičky nejsou stejně velké, ale postupně narůstají. To má za následek, že když do kostičky číslo 3 vrazí ta předchozí, tak ji nedokáže shodit. Teprve když na trojku spadnou zároveň první a druhé domino, tak spadne i to třetí. A tak dále.

I pro silnou indukci platí základní poznatky. Koky (0) a (1) jsou nezávislé, přičemž v základním kroku potvrzujeme přímo platnost dokazovaného, zatímco k indukčním krokům nedokazujeme platnost, ale implikaci neboli posun platnosti. Tyto implikace jsou vždy dělány pro konkrétní n , což je třeba zdůraznit správným zápisem.

△

Příklad 7b.d: Uvažujme tabulky čokolády obdélníkového tvaru, na kterých jsou rýhami naznačeny čtverečky stejné velikosti. Takovou tabulku lze podél rýhy rozlomit a vzniknou dvě tabulky obdélníkového tvaru, přičemž sečtením počtu čtverečků dvou nových tabulek získáme počet čtverečků původní tabulky.

Každou danou tabulku čokolády tak lze postupně dělit na více menších tabulek, až dostaneme jednotlivé čtverečky. Budeme tomu říkat nalámání tabulky. Například u tabulky o rozměrech 2×4 (pořadí řádky, sloupce) můžeme nejprve ulomit jednu řadu podél levé hrany, neboli odломíme tabulku 2×1 a zůstane tabulka 2×3 . Tu první už snadno nalámáme na čtverečky, tu druhou třeba rozdělíme na dvě vodorovné řady 1×3 a tak pokračujeme dál. Ilustruje to následující schéma.



Každé rozdělení představuje lom, tedy na toto nalámání tabulky 2×4 potřebujeme 7 lomů. To samo o sobě není nějak zajímavé, ale zajímavé začne být, když čtenář zkusí i jiné postupy nalámání tabulky 2×4 a zjistí, že všechny způsoby vyžadují 7 lomů. Existuje ještě další tabulka s osmi čtverečky, jmenovitě 1×8 , a také tu můžeme lámat více způsoby a všechny zaberou 7 lomů. Když si čtenář zkusí další tabulky, možná si něčeho všimne.

Tvrdíme, že pokud má původní tabulka n čtverečků, tak nalámání vyžaduje $n - 1$ lomů bez ohledu na konkrétní tvar (obdélníkové) tabulky a na to, v jakém pořadí a jak ty lomy děláme. Zde předpokládáme, že každá menší tabulka se láme zvlášť, není povoleno vzít více tabulek, zlomit je najednou a prohlásit to za jeden lom.

Dokážeme to silnou indukci na počet čtverečků $n \in \mathbb{N}$.

(0) $n = 1$: Tabulku sestávající z jednoho čtverečku není třeba lámat, tedy vyžaduje $0 = 1 - 1$ lomů.

(1) Dáno $n \in \mathbb{N}$. Předpokládejme, že pokud má obdélníková tabulka k čtverečků, kde $1 \leq k \leq n$, pak nalámání vyžaduje $k - 1$ lomů.

Uvažujme tabulku o $n + 1$ čtverečcích. Pak má alespoň dva čtverečky a lze ji tedy rozlomit na dvě části, nechtě jsou jejich velikosti a, b čtverečků. Protože nelze mít prázdnou čokoládu, je určité $a, b \geq 1$, a díky $n + 1 = a + b$ máme také $a \leq n$ a $b \leq n$. Můžeme tedy na oba díly aplikovat indukční předpoklad, první nalámeme pomocí $a - 1$ lomů a druhý pomocí $b - 1$ lomů. Vzniklo tak nalámání původní tabulky, které vyžadovalo úvodní lom plus lámání potomků, celkem

$$1 + (a - 1) + (b - 1) = a + b - 1 = (n + 1) - 1$$

lomů.

□

△

S 7b.2 Poznámka: Pro začátečníka bývá někdy obtížné vybrat správnou indukci. Zatím je to jednoduché, protože máme jen dvě. Nad příkladem přemýšlíme rekurzivně, začneme případem $n + 1$ a snažíme se najít spojitost s přítomností, popřípadě minulostí. Pokud ji najdeme, podíváme se, jaké předchozí případy potřebujeme.

Pokud nám k vyřešení případu $n + 1$ stačí případ n , použijeme slabou indukci. Pokud potřebujeme jít více do minulosti, použijeme silnou indukci.

△

Příklad 7b.e: Uvažujme funkci na \mathbb{N}_0 definovanou takto:

(0_D) $f(0) = 1$;

(1_D) $f(n + 1) = f(0) + f(1) + \dots + f(n) - n = \sum_{k=0}^n f(k) - n$ pro $n \geq 0$.

Nejprve se přesvědčíme, že definice má správnou strukturu, a pokusíme se odhadnout vzorec pro $f(n)$.

$$f(0) \stackrel{(0_D)}{=} 1$$

$$f(1) = f(0 + 1) \stackrel{(1_D)}{=} \sum_{k=0}^0 f(k) - 0 = f(0) - 0 = 1 - 0 = 1$$

$$f(2) = f(1 + 1) \stackrel{(1_D)}{=} \sum_{k=0}^1 f(k) - 1 = f(0) + f(1) - 1 = 1 + 1 - 1 = 1$$

$$f(3) = f(2 + 1) \stackrel{(1_D)}{=} \sum_{k=0}^2 f(k) - 2 = 1 + 1 + 1 - 2 = 1$$

$$f(4) = f(3 + 1) \stackrel{(1_D)}{=} \sum_{k=0}^3 f(k) - 3 = 1 + 1 + 1 + 1 - 3 = 1$$

Také $f(5) = 1$. Zdá se, že $f(n) = 1$. Dokážeme to indukcí. K vyřešení případu $n + 1$ máme jediný zdroj informací, definici (1_D) , a ta se odvolává na všechny předchozí případy, tudíž použijeme silnou indukci.

(0) $n = 0$: $f(0) = 1$ platí.

(1) Dáno $n \geq 0$, IP: Platí $f(k) = 1$ pro $k = 0, \dots, n$.

Pak

$$f(n+1) \stackrel{(1_D)}{=} \sum_{k=0}^n f(k) - n \stackrel{\text{IP}}{=} \sum_{k=0}^n 1 - n = (n+1) - n = 1.$$

□

Indukční předpoklad bychom také mohli napsat takto:

• IP: $f(0) = 1, f(1) = 1, \dots, f(n) = 1$.

Není to sice zcela přesné, ale bývá to tolerováno, protože je to intuitivně názorné.

Začátečníci někdy mají pocit, že se ve vzorci pro $f(n)$ očekává přítomnost toho n , takže zkoušejí věci jako $f(n) = n^0, f(n) = 1^n, f(n) = \frac{n}{n}$ a podobně. Fakticky je to správně, ale dokázat v tomto tvaru indukční implikaci je v zásadě nemožné, protože chybí potřebné identity. K cíli se lze dostat tak, že ony vzorce nahradíme jedničkou a pak se k nim zase v závěru vrátíme, ale pak je jednodušší rovnou dokazovat, že $f(n) = 1$.

△

Nyní ukážeme jednu tradiční aplikaci silné indukce.

Příklad 7b.f: Dokážeme silnou indukci, že každé přirozené číslo větší než 1 je dělitelné nějakým prvočíslem.

(0) $n = 2$: Prvočíslo 2 dělí $n = 2$.

(1) Dáno $n \geq 2$. Předpokládáme, že všechna přirozená čísla mezi 2 a n včetně jsou dělitelná nějakým prvočíslem.

Uvažujme $n + 1$. Pokud je to prvočíslo, tak dělí samo sebe a máme splněno. Pokud $n + 1$ není prvočíslo, pak $n + 1 = a \cdot b$, kde $a, b \in \mathbb{N}$ jsou čísla splňující $1 < a < n + 1$ a $1 < b < n + 1$, takže a je přirozené číslo mezi 2 a n . Podle indukčního předpokladu jej musí dělit nějaké prvočíslo p . Takže p dělí a a to dělí $n + 1$, tedy prvočíslo p dělí $n + 1$ a jsme hotovi.

□

△

M 7b.3 Poznámka: Indukce má vlastně dvě vrstvy. Primární vrstva nesouvisí s tím, co dokazujeme či definujeme, jejím cílem je pomocí vhodného schématu (slabá, silná atd. indukce) projít pomocí specifických kroků všemi čísly zvolené množiny $\{n \in \mathbb{Z}; n \geq n_0\}$. Srdcem slabé indukce tak je pro množinu \mathbb{N} schéma

$$\xrightarrow{(0)} 1 \xrightarrow[n=1]{(1)} 2 \xrightarrow[n=2]{(1)} 3 \xrightarrow[n=3]{(1)} \dots$$

zatímco základem silné indukce je schéma

$$\xrightarrow{(0)} 1 \quad 1 \xrightarrow[n=1]{(1)} 2 \quad \left. \begin{array}{l} 1 \\ 2 \end{array} \right] \xrightarrow[n=2]{(1)} 3 \quad \left. \begin{array}{l} 1 \\ 2 \\ 3 \end{array} \right] \xrightarrow[n=3]{(1)} 4 \quad \text{atd.}$$

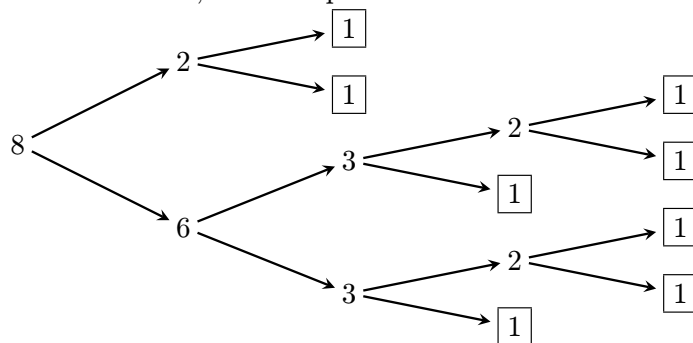
Pro posuny \mathbb{N} pak tato schémata vhodně modifikujeme.

Potkáme také další schémata a pro strukturální správnost indukce je třeba ověřit, že dotyčné schéma opravdu pokryje celou potřebnou množinu. Pokud ano, pak pomocí tohoto schématu můžeme na té množině něco dokazovat nebo vytvářet, což je ta druhá vrstva.

To byl pohled teoretický, kdy zavádíme různá schémata pro indukci. Z pohledu praktického máme nějaké dokazované tvrzení či vytvářený objekt. Prozkoumáním případu $n + 1$ zjistíme, jak souvisí s předchozími, což nás pak navede na vhodné schéma buď již existující, nebo specifické, u kterého ověříme, že pokrývá potřebnou množinu. \triangle

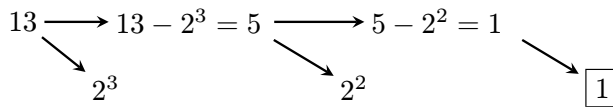
Poznámka: Podívejme se blíže na proces vymýšlení indukce. Již jsme konstatovali, že v důkazech postupujeme od základního kroku k indukčnímu, ale vymýšlíme je spíše rekurzí, tedy pohledem shora dolů či pozpátku. Z podstaty řešeného problému vyplyne mechanismus přechodu od případu $n + 1$ k předchozím, tedy základní schéma, u kterého musíme určit nejen podobu indukčního kroku, ale také u jaké hodnoty rekurze skončí. To je pak základní případ z kroku (0).

Vraťme se k příkladu s čokoládou. Nakreslili jsme schéma pro jedno možné nalámání se symboly tabulek, ale v důkazu jsme pracovali s počtem čtverečků, takže to překreslíme.

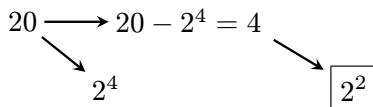


Vidíme, jak rekurzivně přecházíme od větších čísel k menším, dokud neskončíme se základním případem řešeným v kroku (0).

Když se takto podíváme na důkaz v příkladu 7b.a, tak zjistíme, že jsme vlastně k základnímu případu $n = 1$ chodili jen někdy, ale často se naše cesta zastavila dříve. Porovnejme rekurzivní cestu pro dva různé vstupy. Rozklad $13 = 2^3 + 2^2 + 1$ byl obdržén takto:



Ovšem rozklad $20 = 2^4 + 2^2$ proběhl v důkazu takto:



Tato rekurze má tedy reálně vzato nekonečně mnoho základních hodnot typu 2^k , na kterých se zastaví. Byli jsme sice schopni formálně sepsat důkaz tak, aby měl jen jednu oficiální konečnou hodnotu $n = 1$, ale to se nemusí vždycky povést. Navíc je formální podoba sice správná, ale zastírá skutečnou podstatu situace, tedy že máme více základních hodnot.

Podobně při hledání prvočíselného dělitele jsme v mnoha případech z rekurzivního procesu vyskočili dříve, než jsme dojeli k základní hodnotě $n = 2$. Ve skutečnosti jsou zastavovacími hodnotami všechna prvočísla. \triangle

Ukážeme teď situaci, kdy už problém více základních hodnot nelze tak snadno zakrýt, takže nám nezbude, než mu čelit.

Příklad 7b.g: Uvažujme následující induktivní definici posloupnosti F_n pro $n \in \mathbb{N}$:

(0_D) $F_1 = 1, F_2 = 1;$

(1_D) $F_{n+1} = F_n + F_{n-1}$ pro $n \geq 2$.

Nejprve se podíváme, že opravdu vzniká posloupnost.

F_1 a F_2 známe. Pro F_3 potřebujeme použít indukční vzorec, a protože $F_3 = F_{2+1}$, potřebujeme jej použít s volbou $n = 2$, což je v povoleném rozsahu. Dostaneme

$$F_3 = F_{2+1} \stackrel{(1_D)}{=} F_2 + F_{2-1} = F_2 + F_1 = 1 + 1 = 2.$$

Obdobně pak

$$F_4 \stackrel{(1_D)}{=} F_3 + F_2 = 2 + 1 = 3,$$

$$F_5 \stackrel{(1_D)}{=} F_4 + F_3 = 3 + 2 = 5, \dots$$

V této posloupnosti je tedy každý člen součtem dvou předchozích (s výjimkou prvních dvou). Dostáváme tak čísla 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, . . . , což je slavná Fibonacciho posloupnost. V příkladě 10b.d vyložíme, odkud se vzala, zde nás budou zajímat aspekty induktivní či rekurzivní.

Začneme zdánlivým rozporem. Máme posloupnost F_n pro $n \geq 1$, ale indukční vzorec je předepsán pro $n \geq 2$. Tento zjevný nesoulad by u jednoduché indukce indikoval problém, ale u pokročilejší indukce to naopak takto dává smysl. Každé z těchto vymezení totiž specifikuje něco jiného. První říká, které členy posloupnosti existují, druhé zase, které rovnosti v indukčním zápise máme k dispozici. Nemusejí se shodovat, podstatné je, jak na sebe indukční a základní část navazují.

Když jsme výše počítali první hodnoty posloupnosti, tak jsme našli také člen F_1 , tedy specifikace $n \geq 1$ je pro posloupnost správná. Na druhou stranu jsme indukční vzorec pro $n = 1$ nepotřebovali, nejnižší potřebná hodnota byla opravdu pro $n = 2$. Má tedy smysl jej vymežit nerovností $n \geq 2$. Nejen to, pokud bychom se indukční vzorec pokusili použít pro $n = 1$, dostali bychom předpis $F_2 = F_1 + F_0$, který se odvolává na neexistující hodnotu F_0 . Takže vymezení $n \geq 1$ pro indukční vzorec dokonce ani nedává smysl.

Definici tedy rozumíme a možná bychom chtěli o takto vzniklé posloupnosti něco dokázat, třeba že opravdu existuje pro všechna $n \in \mathbb{N}$, nebo že docela rychle roste. Přírozeným nástrojem je indukce. Jakou bude mít podobu?

V poznámce 7b.3 jsme připomněli schémata pro průchod množinou \mathbb{N} pro slabou a silnou indukci. Žádné z nich ale nevyhovuje tomu, jak vzniká Fibonacciho posloupnost, a proto je nelze použít.

Představme si, že se pokoušíme o Fibonacciho posloupnosti něco dokázat indukcí. V indukčním kroku chceme něco zjistit o případě $n + 1$ a jedinou informaci (a zároveň vazbu na předchozí případy) představuje definiční vzorec (1_D). Abychom jej mohli využít, potřebujeme informace o případech n a $n - 1$. Ovšem při slabé indukci nám IP poskytne jen informaci o konkrétní hodnotě n ; jak jsme opakovaně zdůrazňovali, o jiných hodnotách, například $n - 1$, neříká nic. Takže nám nepomůže.

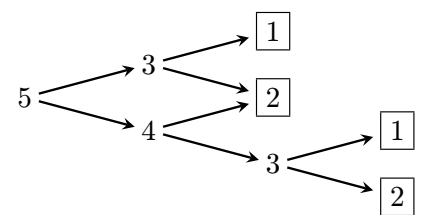
Silná indukce nabízí více informací v předpokladu, ovšem s jednou výjimkou, a to pro první hodnotu $n = n_0$, kde má příslušná implikace zase nedostačující podobu $V(n_0) \implies V(n_0)$. Ani silná indukce proto nebude pro Fibonacciho posloupnost fungovat.

Budeme tedy potřebovat nový typ indukce, který nám v každém indukčním kroku nabídne potřebnou informaci ve formě předpokladu. Budeme potřebovat vždy alespoň dva údaje, tedy n a $n - 1$, a je zbytečné vyžadovat víc. Všechny indukční implikace by tedy mohly mít podobu přechodu $(n, n - 1) \mapsto n + 1$. To má smysl pro $n \geq 2$, protože pro $n = 1$ bychom vyžadovali informaci o neexistujícím F_0 .

Aby se taková indukce „rozjela“, je nutno prokázat v základním kroku splnění indukčních předpokladů v nějakém konkrétním případě, což zde znamená ve dvou po sobě následujících číslech. Nabízí se $n = 1$ a $n = 2$, o kterých máme přímé informace. To vede na následující schéma:

$$\xrightarrow{(0)} \left[\begin{array}{cc} 1 & 1 \\ 2 & 2 \end{array} \right] \xrightarrow[n=2]{(1)} 3 \quad \left[\begin{array}{c} 2 \\ 3 \end{array} \right] \xrightarrow[n=3]{(1)} 4 \quad \left[\begin{array}{c} 3 \\ 4 \end{array} \right] \xrightarrow[n=4]{(1)} 5 \quad \text{atd.}$$

Toto schéma odpovídá tomu, jak vznikají Fibonacciho čísla. Zvolené počáteční hodnoty odpovídají koncovým hodnotám při rekurentním pohledu. Například vpravo vidíme, jaké informace potřebujeme k odvození F_5 . Rekurze skončí u čísel 1 a 2, přesně jak očekáváme.



Dostáváme tak schéma pro průchod množinou \mathbb{N} , které je kompatibilní s Fibonacciho posloupností. Zároveň vidíme, že má stejnou strukturu jako její definice, což není náhoda. Jak posléze uvidíme, je to pravidlo.

Jako ukázkou dokážeme, že Fibonacciho posloupnost opravdu existuje a splňuje odhady $F_n \leq 2^n$ a $F_n \geq \frac{4}{9} \cdot \left(\frac{3}{2}\right)^n$ pro $n \in \mathbb{N}$.

(0) $n = 1$: $F_1 = 1$ existuje dle (0_D) a splňuje $\frac{4}{9} \cdot \frac{3}{2} = \frac{2}{3} \leq 1 = F_1 \leq 2 = 2^1$.

$n = 2$: $F_2 = 1$ existuje dle (0_D) a splňuje $\frac{4}{9} \cdot \left(\frac{3}{2}\right)^2 = 1 \leq F_2 \leq 4 = 2^2$.

(1) Dáno $n \geq 2$. Předpokládejme, že existují čísla F_n a F_{n-1} a obě splňují příslušné odhady. Pak existuje i číslo $F_n + F_{n-1}$ a podle (1_D) tedy existuje i F_{n+1} . Pro něj pak platí potřebný horní odhad:

$$\begin{aligned} F_{n+1} &\stackrel{(1D)}{=} F_n + F_{n-1} \stackrel{IP}{\leq} 2^n + 2^{n-1} && / \quad 2^{n-1} \leq 2^n \\ &\leq 2^n + 2^n = 2 \cdot 2^n = \underline{2^{n+1}}. \end{aligned}$$

Dolní odhad:

$$\begin{aligned} F_{n+1} &\stackrel{(1D)}{=} F_n + F_{n-1} \stackrel{IP}{\geq} \frac{4}{9} \cdot \left(\frac{3}{2}\right)^n + \frac{4}{9} \cdot \left(\frac{3}{2}\right)^{n-1} = \frac{4}{9} \cdot \left(\frac{3}{2}\right)^{n-1} \left(\frac{3}{2} + 1\right) = \frac{4}{9} \cdot \left(\frac{2}{3}\right)^2 \cdot \left(\frac{3}{2}\right)^{n+1} \left(\frac{3}{2} + 1\right) \\ &= \frac{4}{9} \cdot \left(\frac{3}{2}\right)^{n+1} \cdot \left(\frac{2}{3}\right)^2 \cdot \frac{5}{2} = \frac{4}{9} \cdot \left(\frac{3}{2}\right)^{n+1} \cdot \frac{10}{9} \geq \frac{4}{9} \cdot \left(\frac{3}{2}\right)^{n+1} \cdot 1 = \underline{\frac{4}{9} \cdot \left(\frac{3}{2}\right)^{n+1}}. \end{aligned}$$

□

Dolní odhad byl trochu dobrodružnější, ale nakonec to o kousek vyšlo. Zjistili jsme, že F_n roste porovnatelně rychle jako geometrické posloupnosti.

△

Oprávněnost představy, že nové schéma prochází množinou \mathbb{N} , podepřeme zavedením dalšího indukčního principu, který obsluhuje případy, kdy se odvoláváme na minulost pokaždé stejným způsobem, tedy pro vyřešení případu $n + 1$ potřebujeme vždy znát m bezprostředně předchozích údajů pro nějaké $m \in \mathbb{N}$. To znamená nutnost znát případy $n, n-1$ až $n-m+1$. Například pro $m = 4$ bychom potřebovali znát případy $n, n-1, n-2$ a $n-3 = n-4+1$, to souhlasí.

Abychom takovou implikaci

$$[V(n-m+1) \wedge V(n-m+2) \wedge \dots \wedge V(n)] \implies V(n+1)$$

mohli využít, musíme ověřit, že předpoklad lze alespoň jednou splnit, tedy musíme v základním kroku (0) ověřit m po sobě jdoucích případů. Pokud má první z nich číslo n_0 , pak jde o případy $n_0, n_0 + 1, \dots, n_0 + m - 1$.

Zbývá vyřešit návaznost kroků (0) a (1). Pokud v základním kroku ověříme platnost V pro čísla $n_0, n_0 + 1$ až $n_0 + m - 1$, tak jsme schopni splnit předpoklad indukční implikace pro volbu $n = n_0 + m - 1$ a tím se dostaneme k případu $n_0 + m$, což je následující číslo, které potřebujeme. Proto právě tímto $n_0 + m - 1$ začneme důkaz kroku (1).

Souhlasí to s naším příkladem, kde potřebujeme $m = 4$ předchozích hodnot? Řekněme, že dokazujeme platnost V pro $n \geq 13 = n_0$. Pak v základním kroku potřebujeme ověřit čtyři hodnoty, tedy hodnoty 13, 14, 15 a 16, což souhlasí, $16 = 13 + 4 - 1 = n_0 + m - 1$. Když máme ověřeny hodnoty 13 až 16, tak nám implikace z (1) umožní potvrdit 17, což nastane pro volbu $n = 16 = n_0 + m - 1$.

7b.4. Modifikovaný princip matematické indukce.

Nechť $n_0 \in \mathbb{Z}$, nechť $V(n)$ je vlastnost celých čísel, která má smysl pro $n \geq n_0$. Nechť $m \in \mathbb{N}$.

Předpokládejme, že:

(0) platí $V(n_0), V(n_0 + 1), V(n_0 + 2), \dots, V(n_0 + m - 1)$.

(1) Pro každé $n \in \mathbb{Z}, n \geq n_0 + m - 1$ je pravdivá následující implikace: Jestliže platí $V(k)$ pro všechna $k = n - m + 1, n - m + 2, \dots, n$, pak platí také $V(n + 1)$.

Potom $V(n)$ platí pro všechna $n \in \mathbb{Z}, n \geq n_0$.

Nemá smysl se učit toto nazpaměť, podstatné je rozumět systému a správně jej aplikovat.

Poznamenejme, že „modifikovaný princip“ je pracovní název, abychom se na něj mohli v tomto textu odvolávat, tento princip nemá univerzálně přijímané jméno. Řada autorů se při používání tohoto principu odvolává na silnou indukci, ale to není správně, protože silný princip umožňuje jen jednu základní hodnotu.

Podobně jako u silného principu, i bez toho modifikovaného bychom se v zásadě obešli, protože místo práce s vlastností V můžeme zavést pomocnou vlastnost W , která zahrnuje V a navíc si pamatuje potřebnou minulost. S tou pak pracujeme slabou indukci. Ukážeme to pro horní odhad Fibonacciho posloupnosti.

Příklad 7b.h (návrat k 7b.g): Chceme dokázat, že pro $n \geq 1$ platí $F_n \leq 2^n$.

Místo toho dokážeme novou vlastnost $W(n)$, která pro $n \geq 2$ říká, že $F_{n-1} \leq 2^{n-1}$ a $F_n \leq 2^n$. Protože $W(n)$ zahrnuje F_{n-1} , museli jsme se s indexem začít až od dvojky.

Rozyslíme si, že pokud se nám podaří dokázat $W(n)$ pro $n \geq 2$, tak to potvrdí žádaný odhad pro všechna $F_n, n \geq 1$.

Vlastnost $W(n)$ dokážeme slabou indukci.

(0) $n = 2$: Pro platnost $W(2)$ potřebujeme potvrdit, že $F_1 \leq 2^1$ a $F_2 \leq 2^2$, což vyplývá z definice (0_D) .

(1) Dáno $n \geq 2$. Předpokládejme, že platí $W(n)$, tedy $F_{n-1} \leq 2^{n-1}$ a $F_n \leq 2^n$.

Potřebujeme ukázat platnost $W(n + 1)$, tedy že $F_n \leq 2^n$ a $F_{n+1} \leq 2^{n+1}$. První nerovnost máme přímo z IP, druhou dokážeme snadno:

$$\begin{aligned} F_{n+1} &\stackrel{(1_D)}{=} F_n + F_{n-1} \stackrel{\text{IP}}{\leq} 2^n + 2^{n-1} && / \quad 2^{n-1} \leq 2^n \\ &\leq 2^n + 2^n = 2 \cdot 2^n = \underline{2^{n+1}}. \end{aligned}$$

$W(n + 1)$ je ověřeno.

□

Jak vidíme, pomocí pomocné vlastnosti W si opravdu vystačíme se slabou indukci.

△

Již tradičně probereme nejoblíbenější chyby.

S 7b.5 Poznámka: Uvažujme funkci zadanou na \mathbb{N}_0 předpisem

$$(0_D) f(0) = 1, f(1) = -1;$$

$$(1_D) f(n+1) = f(n) + 2f(n-1) \text{ pro } n \geq 1.$$

Laskavý čtenář spočítá několik prvních hodnot, aby se přesvědčil, že indukční krok správně navazuje na základní a opravdu tak vzniká funkce na \mathbb{N}_0 . Při té příležitosti si všimne, že $f(n) = 1$ pro sudá n a $f(n) = -1$ pro lichá n , což lze elegantně zachytit vzorcem $f(n) = (-1)^n$. Následující pokusy o důkaz jsou chybné.

První pokus:

$$(0) f(0) = 1 = (-1)^0 \text{ OK.}$$

$$(1) n \geq 0, \text{ IP: } f(n) = (-1)^n. \text{ Pak}$$

$$f(n+1) \stackrel{(1_D)}{=} f(n) + 2f(n-1) \stackrel{\text{IP}}{=} (-1)^n + 2(-1)^{n-1} = (-1)^n - 2(-1)^n = -(-1)^n = (-1)^{n+1}.$$

□

Vzorec (1_D) je použit správně, nic jiného o $f(n+1)$ nevíme. Základní struktura slabé indukce je sama o sobě také správná (sladění základního a indukčního kroku), chyba je zde v aplikaci indukčního předpokladu. V důkazu se výraz $f(n-1)$ nahradil výrazem $(-1)^{n-1}$ s odkazem na IP, ale tam nic takového není. Je tam jen vzorec $f(n) = (-1)^n$, ten ale předpokládáme pro jedno konkrétní číslo n . To $n-1$ je jiné číslo a pro něj nemáme žádnou informaci.

Poučení: Když chceme něco použít v rekuzi či indukci, musíme to dát do IP, jinak máme smůlu. V tomto případě vidíme nutnost mít IP: $f(n) = (-1)^n$, $f(n-1) = (-1)^{n-1}$, tedy bude třeba použít modifikovaný princip indukce.

Druhý pokus:

$$(0) f(0) = 1 = (-1)^0 \text{ OK.}$$

$$(1) n \geq 0, \text{ IP: } f(n-1) = (-1)^{n-1}, f(n) = (-1)^n. \text{ Pak}$$

$$f(n+1) \stackrel{(1_D)}{=} f(n) + 2f(n-1) \stackrel{\text{IP}}{=} (-1)^n + 2(-1)^{n-1} = (-1)^n - 2(-1)^n = -(-1)^n = (-1)^{n+1}.$$

□

Tentokrát jsou předpoklady použity správně, ale chybné je schéma. Má podobu

$$\begin{array}{c} \xrightarrow{(0)} 0 \\ \phantom{\xrightarrow{(0)}} \end{array} \quad \begin{array}{c} -1 \\ \end{array} \Big] \xrightarrow[(n=0]{(1)} 1 \quad \begin{array}{c} 0 \\ \end{array} \Big] \xrightarrow[(n=1]{(1)} 2 \quad \begin{array}{c} 1 \\ \end{array} \Big] \xrightarrow[(n=2]{(1)} 3 \quad \text{atd.}$$

Hned první indukční krok má vstupní data 0 a -1 , které ovšem neexistuje. Dá se to opravit změnou omezení pro n v kroku (1) na $n \geq 1$, pak první indukční krok znamená přechod $0, 1 \mapsto 2$, který už dává smysl, ale je tu druhý problém. Provedený krok (0) nezajistí splnění těchto IP, takže se indukční kaskáda vůbec nerozjede.

Musíme tedy do kroku (0) přidat ověření pro $n = 1$, čímž konečně vznikne správný důkaz. My se ještě podíváme na jiné populární nesprávné nápady.

Třetí pokus:

$$(0) f(0) = 1 = (-1)^0 \text{ OK. } f(1) = -1 = (-1)^1 \text{ OK.}$$

$$(1) n \geq 1, \text{ IP: } f(n+1) = f(n) + 2f(n-1), f(n) = (-1)^n. \text{ Pak}$$

$$f(n+1) \stackrel{(1_D)}{=} f(n) + 2f(n-1) \stackrel{\text{IP}}{=} (-1)^n + 2(-1)^{n-1} = (-1)^n - 2(-1)^n = -(-1)^n = (-1)^{n+1}.$$

□

Tentokrát je krok (0) dobře, chyby jsou dvě. Jedna je ve schématu, nepracuje s dvojicí $n, n-1$, protože v IP opět chybí vzorec pro $f(n-1)$. Naopak je tam jeden údaj navíc. Induktivní předpis pro $f(n+1)$ nemá v IP co dělat, protože jej nedokazujeme. Je nám dán už v zadání, tudíž není důvod jej ještě předpokládat.

Čtvrtý pokus:

$$(0) f(0) = 1 = (-1)^0 \text{ OK.}$$

$$(1) n \geq 0, \text{ IP: } f(n) = (-1)^n. \text{ Pak}$$

$$f(n+1) = f(n) + 1 \stackrel{\text{IP}}{=} (-1)^n + 1 = \dots$$

□

Chyba: Zde by byla struktura slabé indukce v pořádku, protože ve výpočtu se $f(n-1)$ nepoužívá. Zato se tam použila identita $f(n+1) = f(n) + 1$, o které nevíme, zda platí, a tudíž je celý výpočet špatně. Mimochodem, neplatí. Někdy potkávám zajímavou alternativu $f(n+1) = f(n) + f(1)$, která naznačuje, že autor pokusu o důkaz potkal lineární algebru a pojem linearity na něj udělal dojem. Bohužel, o naší f nevíme, zda je lineární (mimochodem není). My si prostě nemůžeme jen tak nějaký vzorec pro $f(n+1)$ vymyslet, musíme vycházet z toho, co je prokazatelně známo. V těchto situacích to je vztah (1_D) z definice.

△

Problém s různými principy indukce je v tom, že jak záhy zjistíme, ani tyto tři nemusejí stačit. Je tedy perspektivnější se naučit rozumět indukci a pak ji přizpůsobovat konkrétním situacím. K tomu zde postupně směřujeme,

nicméně začátečníkům pomůže mít připravené scénáře. Další speciality už nebudeme vymýšlet, takže můžeme shrnout postup.

S Algoritmus 7b.6.

pro dokazování indukci (pro začátečníky).

1. Ujasníme si, co vlastně chceme dokazovat, napíšeme to jako vlastnost $V(n)$ závisující na celočíselném parametru n , kde se n bere pro všechna $n \geq n_0$ a $n_0 \in \mathbb{Z}$ je startovací hodnota.
2. Napíšeme tvrzení $V(n+1)$ a zkusíme najít způsob, jak tento případ převést na nějaké předchozí případy neboli jak se dostat k $V(n+1)$ pomocí nějakých $V(k)$ pro $k \leq n$.
3. Podle 2 se rozhodneme, kterou verzi indukce použijeme. Pokud k potvrzení $V(n+1)$ stačí $V(n)$, je slabý princip nejlepší. Pokud potřebujeme více předchozích hodnot, ale vždy stačí znát m bezprostředně předcházejících, použijeme modifikovaný princip. Pokud se vracíme do minulosti tak, že nestačí znát stále stejný počet bezprostředně předchozích dat, a pro $n_0 + 1$ nám stačí n_0 , pak použijeme silný princip indukce.
4. Rozmyslíme si, které hodnoty musíme znát na počátku, aby se proces indukce mohl rozběhnout. Pro slabý a silný princip to bude hodnota n_0 , pro modifikovaný princip to bude m následných hodnot počínaje n_0 . Pak si rozmyslíme, která hodnota n_1 nám pro $n_1 + 1$ dá první neznámé číslo po základních hodnotách. Tím je určen rozsah pro indukční krok.
5. Provedeme vlastní důkaz:
 - (0) Dokážeme platnost $V(n)$ pro počáteční hodnoty rozmyšlené v bodě 4;
 - (1) Zvolíme libovolné $n \geq n_1$ (viz 4), stanovíme indukční předpoklad a s jeho pomocí dokážeme platnost $V(n+1)$. Pokud dokazujeme rovnost či nerovnost, pak se doporučuje metoda cesty.
6. Zkontrolujeme, že důkaz v části 5 (1) je správný, tedy vychází z toho, co předpokládáme jako pravdivé, a po korektních krocích končí tím, co chceme dokázat.

△

Příklad 7b.i: Uvažujme následující funkci na \mathbb{N} :

$$(0_D) f(1) = 2, f(2) = 3, f(3) = 4;$$

$$(1_D) f(n+1) = f(n) - f(n-2) + n \text{ pro } n \geq 3.$$

Nejprve se přesvědčíme, že definice je správně. Po akceptování základních hodnot je první neznámou hodnotou $f(4)$. Tu získáme jako $f(3+1)$, tedy chceme požit (1_D) pro $n = 3$. Tato hodnota je povolena, je to v pořádku. Je také nejmenší předepsaná, takže předpis v (1_D) neplýtvá zbytečnými vzorci typu $f(3) = f(2) - f(0) + 2$ pracujícími z neexistujícími daty.

$$f(1) \stackrel{(0_D)}{=} 2$$

$$f(2) \stackrel{(0_D)}{=} 3$$

$$f(3) \stackrel{(0_D)}{=} 4$$

$$f(4) = f(3+1) \stackrel{(1_D)}{=}_{n=3} f(3) - f(1) + 3 = 4 - 2 + 3 = 5$$

$$f(5) \stackrel{(1_D)}{=}_{n=4} f(4) - f(2) + 4 = 5 - 3 + 4 = 6$$

Vypadá to, že $f(n) = n + 1$. Potvrdíme to indukci.

Rozbor: Případ $n+1$ se ptá na $f(n+1)$ a jediná informace o tomto objektu se nalézá v definici (1_D) . Ta vyžaduje znalost případů n a $n-2$. Jde o konstantní počet a je jich víc než jen n , což ukazuje na modifikovaný princip indukce. Ten pracuje s celým blokem čísel, zatímco my zde máme mezeru, v požadavcích chybí $n-1$. Naštěstí nemusíme vymýšlet nový princip, můžeme formálně odvozovat případ $n+1$ od případů $n, n-1, n-2$ s tím, že tu prostřední informaci není povinné využít. Máme tedy $m = 3$ kusů informace v indukčním předpokladu a tudíž také budeme ověřovat tři hodnoty v základním kroku.

Protože funkce existuje pro $n \geq 1$, v kroku (0) zpracujeme hodnoty $n = 1, 2, 3$. Tyto hodnoty pak zaručí splnění indukčního předpokladu pro první relevantní implikaci v kroku (1), což odpovídá implikaci (symbolicky) $[1, 2, 3] \implies 4$ a volbě $n = 3$. Krok (1) tedy budeme dokazovat pro $n \geq 3$.

Všimneme si, že toto nastavení důkazu přesně odpovídá struktuře v definici, na což už si začínáme zvykat.

Indukční předpoklad by měl poskytnout vzorec $f(n) = n + 1$ také ve verzi pro $n-1$ a $n-2$, což snadno spočítáme, kolik má vyjít: $f(n-1) = (n-1) + 1 = n$, $f(n-2) = (n-2) + 1 = n-1$. Jdeme na to.

$$(0) f(1) \stackrel{(0_D)}{=} 2 = \underline{1+1}, f(2) \stackrel{(0_D)}{=} 3 = \underline{2+1}, f(3) \stackrel{(0_D)}{=} 4 = \underline{3+1}.$$

$$(1) \text{ Dáno } n \geq 3, \text{ IP: } f(n) = n + 1, f(n-1) = n, f(n-2) = n-1.$$

Pak

$$\underline{f(n+1)} \stackrel{(1_D)}{=} f(n) - f(n-2) + n \stackrel{\text{IP}}{=} n+1 - (n-1) + n = n+2 = \underline{(n+1)} + 1.$$

□

Podobně bychom dokazovali nerovnosti, ale pak musíme čekat, že po aplikaci indukčního předpokladu nevyjde přímo správný výraz, ale bude ještě třeba upravovat.

Zrovna u této funkce by bylo dokazování nerovností velmi problematické. Například odhad $f(n) \geq n$ jistě platí. Teď si představme, že chceme aplikovat indukční předpoklad $f(n) \geq n$, $f(n-2) \geq n-2$ na výraz

$$f(n) = f(n) - f(n-2) + n.$$

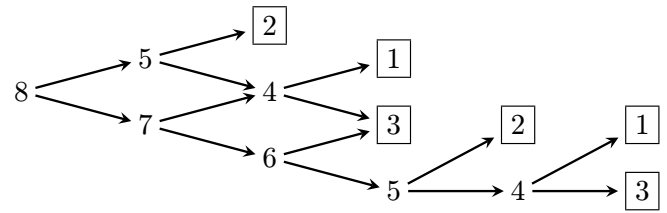
Když $f(n)$ nahradíme výrazem n , tak se podle IP náš výraz zmenší, na druhou stranu když $f(n-2)$ nahradíme výrazem $n-2$, tak se kvůli odčítání náš výraz zvětší. Aplikace IP tak $f(n+1)$ zároveň zvětší i zmenší a vůbec tedy nevíme, co se s ním stane. Indukce proto nebude fungovat.

△

Poznámka: V důkazu jsme do IP přidali nepotřebný případ $n-1$, kvůli tomu jsme pak museli mít tři případy v základním kroku. Nepřidělali jsme si zbytečnou práci?

Pokud bychom zkusili základní hodnoty $n=1$, $n=3$ a indukční krok $[n, n-1] \mapsto n+1$, tak se od 1, 3 pomocí (1) dostaneme k $n=4$, ale neumíme se dostat k číslu 5, protože nemáme ověřena vstupní data pro krok $[2, 4] \mapsto 5$.

Z pohledu rekurze si pak můžeme rozmyslet, že když začínáme s různými čísly n , tak při rekurzi končíme s koncovými hodnotami 1, 2 a 3. Všechny tedy opravdu potřebujeme v základním kroku. Viz příklad pro $n=8$ napravo.



Je možné vytvářet speciální indukční principy, které obslouží případy, kdy v rekurzi přeskakujeme, ale zejména pro začátečníka není snadné odchytil správně všechny základní případy. Aplikace modifikovaného principu je z tohoto pohledu bezpečnější.

△

Příklad 7b.j:

Větu o dělení se zbytkem (1a.26) jsme dokázali pomocí existence nejmenšího prvku a jádrem bylo následující tvrzení:

Je dáno $d \in \mathbb{N}$. Pro každé $n \in \mathbb{N}_0$ existuje $r \in \mathbb{N}_0$ a $q \in \mathbb{Z}$ takové, že $n = qd + r$ a $r < d$.

Tento zbytek r se v praxi dá hledat tak, že od n postupně odečítáme d , což je rekurzivní postup. Funkčnost zpětného kroku je založena na myšlence, že čísla n a $n-d$ mají stejný zbytek po dělení. To nabízí možnost dokázat existenci zbytku pomocí indukce. Z případu $n+1$ chceme přejít k případu $(n+1)-d$. Rozmyslíme si, že ať začneme s jakýmkoliv číslem $n \in \mathbb{N}_0$, rekurze skončí v některém z čísel 0 až $d-1$.

Dospějeme k tomu i formálně. Chceme ukázat existenci zbytku pro $n \geq 0$ a v rekurzi se vždy vracíme o d zpět, což nám formálně umožní modifikovaný princip indukce, kde k případu $n+1$ máme k dispozici předchozích d hodnot. To pak vyžaduje ověřit v základním kroku d základních hodnot, což souhlasí s předchozím pozorováním. Protože tím získáme zbytek pro čísla $0, 1, \dots, d-1$, budeme jako další indukčním krokem získávat číslo $d = n+1$, tedy indukční krok budeme dělat pro $n \geq d-1$.

(0) Pro $n = 0, 1, \dots, d-1$ zvolíme $r = n$, pak $r \in \mathbb{N}_0$, $r < d$ a $n = 0 \cdot d + r$, kde $0 \in \mathbb{Z}$.

(1) Dáno $n \geq d-1$. Předpoklad: Dělení se zbytkem funguje pro čísla $n-d+1$ až n .

(Všimneme si, že díky $n \geq d-1$ platí $n-d+1 \geq 0$, tedy čísla z IP jsou z \mathbb{N}_0 , tedy nedostáváme se do čísel, se kterými naše indukce nepracuje. Navíc pro $n = d-1$ jsou v IP 0 až $d-1$, pro která máme dělení se zbytkem potvrzeno v kroku (0), tedy tato indukce je správně sestavena.)

Uvažujme $n+1$. Pak podle IP existují $r \in \mathbb{N}_0$, $r < d$ a $q \in \mathbb{Z}$ takové, že $n+1-d = qd + r$. Odtud $n+1 = (q+1)d + r$, přičemž $r \in \mathbb{N}_0$, $r < d$ a $q+1 \in \mathbb{Z}$. Dělení se zbytkem je potvrzeno pro $n+1$,

□

△

Důkaz by zkrátilo, kdybychom vymysleli následující princip pro $d \in \mathbb{N}$:

(0) Platí $V(n_0)$ až $V(n_0 + d - 1)$ (celkem d případů);

(1) Pro $n \geq n_0 + d - 1$ platí implikace $V(n-d+1) \implies V(n+1)$.

Tento indukční krok by šlo ekvivalentně přepsat do formálně jednodušší podoby

(1) Pro $n \geq n_0 + d$ platí $V(n-d) \implies V(n)$,

popřípadě populární

(1) Pro $n \geq n_0$ platí implikace $V(n) \implies V(n+d)$.

Není ale zvykem takovýto princip zavádět. Pokročilí indukčníci jsou nad „standardní“ schémata povzneseni a vytvářejí si (správná) schémata dle potřeby, zatímco začátečníkům stačí modifikovaný princip. Ukážeme ještě jeden populární příklad na indukci, která se přesouvá o jeden konstantní krok.

Příklad 7b.k: Představme si, že máme k dispozici mince s hodnotami 3 a 5.

Poznámka: Tříkoruny opravdu existovaly, od roku 1953 papírová, od roku 1965 kovová, ta pak byla roku 1972 zrušena (protože si Němci stěžovali, že ji lze v jejich automatech používat místo mnohem hodnotnější mince germánské).

Zaplacení částky $n \in \mathbb{N}$ (což děláme třeba u pokladny v obchodě) probíhá tak, že zákazník předá nějaké peníze, pokladník také předá nějaké peníze a rozdíl je n .

Tvrdíme, že pomocí tříkorun a pětikorun zaplatíme libovolnou částku $n \in \mathbb{N}$. Dokážeme to indukcí, a to slabou.

(0) $n = 1$: Dáme dvě tříkoruny, dostaneme pětikorunu a zaplatili jsme $n = 1$ korunu.

(1) Dáno $n \geq 1$, předpokládáme, že umíme zaplatit n korun.

Pak tedy zaplatíme n korun, přidáme dvě tříkoruny, dostaneme zpět pětikorunu a zaplatili jsme $n + 1$ korun.

□

V některých situacích je ale potřeba částku n vyplatit, tedy dáme někomu nějaké mince v součtu n . Tvrdíme, že tříkorunami a pětikorunami je možné vyplatit libovolnou částku alespoň 8 korun.

Rozbor: Vyplacení částky $n + 1$ lze převést na předchozí případ odebráním tříkoruny, čímž vznikne případ $n - 2$. Protože se vracíme zpět o konstantní hodnotu, bude možné aplikovat modifikovanou indukci s předpokladem o číslech $n - 2$, $n - 1$, n . Budeme tedy muset v základním kroku zvládnout také tři hodnoty, jmenovitě 8, 9, 10. První další neznámou hodnotou je 11, což se získá indukčním krokem volbou $n = 10$, tím začne krok (1).

(0) Ověříme: $8 = 3 + 5$, $9 = 3 + 3 + 3$, $10 = 5 + 5$.

(1) Nechť $n \geq 10$, předpokládejme, že umíme pomocí tříkorun a pětikorun vyplatit částky $n - 2$, $n - 1$, n . Když k částce $n - 2$ přidáme tříkorunu, tak jsme vyplatili částku $n + 1$.

□

Začali jsme osmičkou, protože 7 není možné vyplatit pomocí tříkorun a pětikorun. Umíme ale vyplatit 6. Když zkusíme několik rekurentních běhů pro různé částky, tak zjistíme, že je možné při zpětném skákání po trojkách pracovat s koncovými stavy 3, 5, 10. Pokud bychom je zpracovali v kroku (0), tak by indukční krok (1) potvrdil vyplatitelnost částek z množiny

$$\{3, 5, 6, 8, 9, 10, 11, 12, 13, \dots\} = \{3, 5, 6\} \cup \{n \in \mathbb{N}; n \geq 8\}.$$

Bylo by to sice matematicky obecnější a korektní, ale nezní to tak pěkně jako naše původní tvrzení.

△

Příklad 7b.l: Uvažujme následující posloupnost a_n pro $n \geq 1$:

(0_D) $a_1 = 1$, $a_2 = 2$;

(1_D) $a_{n+1} = \frac{2}{n} \sum_{k=1}^n a_k = \frac{2}{n} [a_1 + \dots + a_n]$ pro $n \geq 2$.

Jak tato posloupnost vypadá?

$$a_1 \stackrel{(0_D)}{=} 1;$$

$$a_2 \stackrel{(0_D)}{=} 2;$$

$$a_3 = a_{2+1} \stackrel{(1_D)}{=} \frac{2}{n=2} \frac{2}{2} [a_1 + a_2] = 3;$$

$$a_4 \stackrel{(1_D)}{=} \frac{2}{n=3} \frac{2}{3} [a_1 + a_2 + a_3] = 4;$$

$$a_5 \stackrel{(1_D)}{=} \frac{2}{n=4} \frac{2}{4} [a_1 + a_2 + a_3 + a_4] = 5; \dots$$

Výpočty ukazují, že indukční definice (1_D) správně navazuje na základní krok definice, zejména rozsah $n \geq 2$ pro (1_D) je zvolen správně. Výsledky také naznačují, že $a_n = n$ pro $n \in \mathbb{N}$. Zkusíme to dokázat indukcí.

Rozbor: Pro vyřešení případu $n + 1$ potřebujeme znát všechny předchozí případy, takže slabý ani modifikovaný princip inkluze nelze použít. Zbývá silný princip, ale ten umožňuje jen jednu startovací hodnotu, což není tento případ. Budeme tedy muset vymyslet specifické schéma a zkušenost naznačuje, že by mělo strukturu odpovídat

definici. Množinou \mathbb{N} by nás tedy měly provést následující kroky:

$$\xrightarrow{(0)} \left[\begin{array}{c} 1 \\ 2 \end{array} \right] \xrightarrow[n=2]{(1)} 3 \quad \left[\begin{array}{c} 1 \\ 2 \\ 3 \end{array} \right] \xrightarrow[n=3]{(1)} 4 \quad \left[\begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} \right] \xrightarrow[n=4]{(1)} 5 \quad \text{atd.}$$

Důkaz proto bude vypadat takto:

(0) $a_1 \stackrel{(0_D)}{=} 1$, $a_2 \stackrel{(0_D)}{=} 2$ souhlasí.

(1) Pro zvolené $n \geq 2$ předpokládejme, že $a_1 = 1$, $a_2 = 2$ až $a_n = n$.

Pak

$$\underline{a_{n+1}} \stackrel{(1_D)}{=} \frac{2}{n} \sum_{k=1}^n a_k \stackrel{\text{IP}}{=} \frac{2}{n} \sum_{k=1}^n k = \frac{2}{n} \cdot \frac{1}{2} n(n+1) = \underline{n+1}.$$

□

Jak víme, že to funguje? Mohli bychom formálně vytvořit další formu indukce, něco jako supersilná indukce, ale není to zvykem a není to perspektivní. Spíše se zamysleme nad obecnými souvislostmi indukce, což si zaslouží vlastní sekci.

Pro úplnost dodejme, že jako obvykle by platnost vzorce $a_n = n$ šlo potvrdit slabou indukcí aplikovanou na umělou vlastnost $W(n)$, která by zachycovala celou minulost.

Formálně, definovali bychom $W(n)$ jako vlastnost $a_k = k$ pro $k \in \{1, \dots, n\}$.

Tuto vlastnost bychom pak dokázali pro $n \geq 2$, přičemž základní krok, tedy platnost $W(2)$ neboli platnost $a_1 = 1$ a $a_2 = 2$ je zaručena krokem (0_D) z definice.

△

Cvičení

Cvičení 7b.1 (rutinní): Uvažujte následující funkce definované indukcí. Pro každou spočítejte f ve třech hodnotách, které následují po těch určených v základním kroku.

- a) (0) $f(0) = -2$, $f(1) = 1$; (1) $f(n+1) = f(n) - 2f(n-1)$ pro $n \in \mathbb{N}$;
 b) (0) $f(1) = 2$; (1) $f(n+1) = f(1) + \dots + f(n)$ pro $n \in \mathbb{N}$;
 c) (0) $f(0) = 1$, $f(1) = -2$; (1) $f(n+1) = f(n-1)^2 f(n) + n$ pro $n \in \mathbb{N}$;
 d) (0) $f(2) = 1$, $f(3) = -2$; (1) $f(n+1) = \frac{f(n-1)}{f(n)}$ pro $n \geq 3$.

Cvičení 7b.2 (poučné): Která z následujících definic funkce na \mathbb{N}_0 je korektní?

- a) $f(0) = 1$; (1) $f(n+1) = f(n) - f(n-1)$ pro $n \geq 1$;
 b) $f(0) = 1$, $f(1) = -1$; (1) $f(n+1) = f(n) - f(n-1)$ pro $n \geq 2$;
 c) $f(0) = 1$, $f(1) = -1$; (1) $f(n+1) = f(n) - f(n-1)$ pro $n \geq 1$.

Cvičení 7b.3 (poučné): Uvažujme následující důkaz, že každé $n \geq 2$ je sudé:

(0) $n = 2$: Dvojka je sudá.

(1) $n \geq 2$, IP: n a $n-1$ jsou sudé. Pak $n+1 = 2 \cdot n - (n-1)$ je coby rozdíl dvou sudých čísel sudé.

Kde je chyba?

Cvičení 7b.4 (rutinní, poučné, zkouškové): Uvažujte funkce definované induktivně následujícími vzorci. Pro každou z nich spočítejte několik hodnot a zkuste odhadnout, jakým vzorcem je $f(n)$ dáno. Pak dokažte, že je to správně.

Soustředte se na správnou volbu typu indukce a zapsání důkazu.

- a) (0) $f(1) = 1$, $f(2) = 2$, $f(3) = 3$; (1) $f(n+1) = f(n) + f(n-1) - f(n-2)$ pro $n \geq 3$;
 b) (0) $f(0) = 0$; (1) $f(n+1) = f(n) + 2n + 1$ pro $n \geq 0$;
 c) (0) $f(1) = 1$; (1) $f(n+1) = \prod_{k=1}^n f(k) = f(1) \cdots f(n)$ pro $n \geq 1$;
 d) (0) $f(0) = 1$, $f(1) = 2$; (1) $f(n+1) = f(n) + 2f(n-1)$ pro $n \geq 1$.

Cvičení 7b.5 (rutinní, poučné): Uvažujte funkce definované na \mathbb{N}_0 induktivně následujícími vzorci. Pro každou z nich spočítejte několik hodnot a zkuste odhadnout, jakým vzorcem je $f(n)$ dáno. Pak dokažte, že je to správně.

- a) (0) $f(0) = 0$; (1) $f(n+1) = \sum_{k=0}^n f(k) = f(0) + \dots + f(n)$ pro $n \geq 0$;
 b) (0) $f(0) = 0$; (1) $f(n+1) = \prod_{k=0}^n f(k) = f(0) \cdots f(n)$ pro $n \geq 0$.

Cvičení 7b.6 (rutinní, zkouškové, *dobré): Uvažujte funkce definované induktivně následujícími vzorci. Pro každou z nich spočítejte několik hodnot a zkuste odhadnout, jakým vzorcem je $f(n)$ dáno. Pak dokažte, že je to správně.

- a) (0) $f(1) = 1, f(2) = 2$; (1) $f(n+1) = 2f(n) - f(n-1)$ pro $n \geq 2$;
 b) (0) $f(1) = 1, f(2) = 1, f(3) = 1$; (1) $f(n+1) = f(n) + f(n-1) - f(n-2)$ pro $n \geq 3$;
 c) (0) $f(0) = 1, f(1) = 4$; (1) $f(n+1) = f(n) + 4f(n-1) + 2 \cdot 4^n$ pro $n \geq 1$;
 d) (0) $f(1) = -1, f(2) = 1$; (1) $f(n+1) = f(n-1) \cdot |f(n)|$ pro $n \geq 2$;
 e)* (0) $f(1) = 1, f(2) = 0, f(3) = 1$; (1) $f(n+1) = f(n) + f(n-1) - f(n-2)$ pro $n \geq 3$;
 f)* (0) $f(0) = 1, f(1) = 3$; (1) $f(n+1) = \begin{cases} 3f(n), & n \in \mathbb{N} \text{ liché;} \\ 9f(n-1), & n \in \mathbb{N} \text{ sudé;} \end{cases}$
 g)* (0) $f(1) = 1, f(2) = 2$; (1) $f(n+1) = 2f(n-1)$ pro $n \geq 2$;
 h)* (0) $f(0) = 1, f(1) = 0, f(2) = 2$, (1) $f(n) = 2f(n-3)$ pro $n \geq 3$.

Cvičení 7b.7 (rutinní, zkouškové): Uvažujte funkce definované induktivně následujícími vzorci. Pro každou z nich dokažte zadanou (ne)rovnost.

Poznámka: Neztrácejte čas snahou uhodnout explicitní vzorec pro $f(n)$.

- a) (0) $f(1) = 1, f(2) = 2$; (1) $f(n+1) = f(n) + n f(n-1)$ pro $n \geq 2$; nerovnost $f(n) \leq n!$;
 b) (0) $f(1) = 1, f(2) = 2$; (1) $f(n+1) = \frac{1}{n} f(n) + f(n-1)$ pro $n \geq 2$; nerovnost $f(n) \leq n^2$;
 c) (0) $f(1) = 1, f(2) = 2$; (1) $f(n+1) = n f(n) + n f(n-1)$ pro $n \geq 2$; rovnost $f(n) = n!$;
 d) (0) $f(1) = 2, f(2) = 3$; (1) $f(n+1) = n f(n) + n^2 f(n-1)$ pro $n \geq 2$; nerovnost $f(n) \geq n!$;
 e) (0) $f(1) = 1, f(2) = 2, f(3) = 3$; (1) $f(n+1) = f(n-2) + f(n-1) + f(n)$ pro $n \geq 3$; nerovnost $f(n) \leq 2^n$.

Cvičení 7b.8 (rutinní, poučné): Uvažujme posloupnost danou předpisem

$$(0) F_1 = F_2 = 1.$$

$$(1) F_{n+1} = F_n + F_{n-1} \text{ pro } n \geq 2.$$

(Je to tzv. Fibonnaciho posloupnost, viz příklad 7b.g a 10b.d.)

A) Odhadněte, která F_n jsou lichá, a dokažte to.

B) Dokažte následující vztahy:

$$a) F_1^2 + F_2^2 + \dots + F_n^2 = F_n F_{n+1} \text{ pro } n \in \mathbb{N};$$

$$b) F_1 + F_3 + \dots + F_{2n-1} = F_{2n} \text{ pro } n \in \mathbb{N};$$

$$c) F_{n+1} F_{n-1} - F_n^2 = (-1)^n \text{ pro } n \in \mathbb{N};$$

$$d) F_1 F_2 + \dots + F_{2n-1} F_{2n} = F_{2n}^2 \text{ pro } n \in \mathbb{N};$$

$$e) F_1 - F_2 + \dots + F_{2n-1} - F_{2n} = 1 - F_{2n-1} \text{ pro } n \in \mathbb{N};$$

$$f) F_k F_n + F_{k+1} F_{n+1} = F_{n+k+1} \text{ pro } n, k \in \mathbb{N};$$

$$g) \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & 0 \end{pmatrix} \text{ pro } n \in \mathbb{N}.$$

Cvičení 7b.9 (poučné): Dokažte, že každé přirozené číslo lze napsat ve tvaru $n = 2^m l$, kde $m \in \mathbb{N}_0$ a l je liché. Náповěda: Čísla jsou sudá a lichá.

Cvičení 7b.10 (poučné): Dokažte, že každý konvexní n -úhelník pro $n \geq 3$ má součet vnitřních úhlů roven $(n-2)\pi$.

Poznámka: n -úhelník má n vrcholů, stran a vnitřních úhlů. Konvexní znamená, že všechny vnitřní úhly jsou ostré. Náповěda: Pro $N \geq 4$ lze konvexní N -úhelníky rozdělit nějakou úhlopříčkou na dva konvexní úhelníky. Nakreslete si to, abyste viděli, co se stane s úhly.

Řešení:

7b.1: a) $f(2) = f(1) - 2f(0) = 5, f(3) = f(2) - 2f(1) = 3, f(4) = -7$. b) $f(2) = f(1) = 2, f(3) = f(1) + f(2) = 4, f(4) = f(1) + f(2) + f(3) = 8$.

c) $f(2) = f(0)^2 f(1) + 1 = -1, f(3) = f(1)^2 f(2) + 2 = -2, f(4) = f(2)^2 f(3) + 3 = 1$. d) $f(4) = \frac{f(2)}{f(3)} = -\frac{1}{2}, f(5) = \frac{f(3)}{f(4)} = 4, f(6) = -\frac{1}{8}$.

7b.2: a) chybná, málo dat v (0). b) chybná, (1) musí začít od $n \geq 1$. c) správná.

7b.3: V IP máme dva údaje, ale v (0) ověříme jen jeden.

7b.4: a) $f(n) = n$ modifikovaná MI. (0) $n = 1, 2, 3$: OK. (1) $n \geq 3$, IP: $f(n) = n, f(n-1) = n-1, f(n-2) = n-2$.

Pak $f(n+1) \stackrel{(1D)}{=} f(n) + f(n-1) - f(n-2) \stackrel{IP}{=} n + (n-1) - (n-2) = n+1$.

b) $f(n) = n^2$ slabá MI. (0) $n = 0$: OK. (1) $n \geq 0$, IP: $f(n) = n^2$. Pak $f(n+1) \stackrel{(1D)}{=} f(n) + 2n + 1 \stackrel{IP}{=} n^2 + 2n + 1 = (n+1)^2$.

c) $f(n) = 1$ silná MI (0) $n = 1$: OK. (1) $n \geq 1$, IP: $f(k) = 1$ pro $1 \leq k \leq n$. Pak $f(n+1) \stackrel{(1D)}{=} f(1) \cdots f(n) \stackrel{IP}{=} 1 \cdots 1 = 1$ nebo $f(n+1) \stackrel{(1D)}{=} \prod_{k=1}^n f(k) \stackrel{IP}{=} \prod_{k=1}^n 1 = 1$.

d) $f(n) = 2^n$ modifikovaná MI. (0) $n = 0, 1$: OK. (1) $n \geq 1$ IP: $f(n) = 2^n$, $f(n-1) = 2^{n-1}$. Pak $f(n+1) \stackrel{(1D)}{=} f(n) + 2f(n-1) \stackrel{IP}{=} 2^n + 2 \cdot 2^{n-1} = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$.

7b.5: a) $f(n) = 0$ (0) $n = 0$: OK. (1) $n \geq 0$, IP: $f(k) = 0$ pro $0 \leq k \leq n$. Pak $f(n+1) \stackrel{(1D)}{=} f(0) + \dots + f(n) \stackrel{IP}{=} 0 + \dots + 0 = 0$ nebo $f(n+1) \stackrel{(1D)}{=} \sum_{k=0}^n f(k) \stackrel{IP}{=} \sum_{k=1}^n 0 = 0$.

b) $f(n) = 0$ (0) $n = 0$: OK. (1) $n \geq 0$, IP: $f(k) = 0$ pro $0 \leq k \leq n$. Pak $f(n+1) \stackrel{(1D)}{=} f(0) \cdot \dots \cdot f(n) \stackrel{IP}{=} 0 \cdot \dots \cdot 0 = 0$ nebo $f(n+1) \stackrel{(1D)}{=} \prod_{k=0}^n f(k) \stackrel{IP}{=} \prod_{k=1}^n 0 = 0$.

7b.6: a) $f(n) = n$. (0) $n = 1$ a $n = 2$ OK. (1) $n \geq 2$, IP: $f(n) = n$ a $f(n-1) = n-1$. Pak $f(n+1) = 2f(n) - f(n-1) \stackrel{IP}{=} 2n - (n-1) = n+1$.

b) $f(n) = 1$. (0) $n = 1, n = 2$ a $n = 3$ OK. (1) $n \geq 3$, IP: $f(n) = 1$, $f(n-1) = 1$ a $f(n-2) = 1$. Pak $f(n+1) = f(n) + f(n-1) - f(n-2) \stackrel{IP}{=} 1 + 1 - 1 = 1$.

c) $f(n) = 4^n$. (0) $n = 0$ a $n = 1$ OK. (1) $n \geq 1$, IP: $f(n) = 4^n$ a $f(n-1) = 4^{n-1}$. Pak $f(n+1) = f(n) + 4f(n-1) + 2 \cdot 4^n \stackrel{IP}{=} 4^n + 4 \cdot 4^{n-1} + 2 \cdot 4^n = 4 \cdot 4^n = 4^{n+1}$.

d) $f(n) = (-1)^n$. (0) $n = 1$ a $n = 2$ OK. (1) $n \geq 2$, IP: $f(n) = (-1)^n$ a $f(n-1) = (-1)^{n-1}$. Pak $f(n+1) = f(n-1) \cdot |f(n)| \stackrel{IP}{=} (-1)^{n-1} \cdot |(-1)^n| = (-1)^{n-1} = (-1)^{n+1}$.

e) $f(n) = \begin{cases} 1, & n \text{ liché;} \\ 0, & n \text{ sudé.} \end{cases}$ (0) Pro $n = 1, 2, 3$ OK.

(1) $n \geq 3$, IP: $f(k) = \begin{cases} 1, & k \text{ liché;} \\ 0, & k \text{ sudé} \end{cases}$ pro $k = n-2, n-1, n$.

Je-li n sudé, pak $n-2$ je sudé, zato $n-1$ a $n+1$ jsou liché. Pak $f(n+1) = f(n) + f(n-1) - f(n-2) \stackrel{IP}{=} 0 + 1 - 0 = 1$, souhlasí pro liché $n+1$.

Je-li n liché, pak $n-2$ je liché, zato $n-1$ a $n+1$ jsou sudé. Pak $f(n+1) = f(n) + f(n-1) - f(n-2) \stackrel{IP}{=} 1 + 0 - 1 = 0$, souhlasí pro sudé $n+1$.

Alternativa: $f(n) = \frac{1}{2}(1 - (-1)^n)$, pak lze přímo, z indukčního předpokladu vyjde

$f(n+1) = f(n) + f(n-1) - f(n-2) \stackrel{IP}{=} \frac{1}{2}(1 - (-1)^n) + \frac{1}{2}(1 - (-1)^{n-1}) - \frac{1}{2}(1 - (-1)^{n-2}) = \frac{1}{2}(1 - (-1)^n + 1 + (-1)^n - 1 + (-1)^n) = \frac{1}{2}(1 + (-1)^n) = \frac{1}{2}(1 - (-1)^{n+1})$.

f) $f(n) = 3^n$. (0) $n = 1$ a $n = 2$ OK. (1) $n \in \mathbb{N}$, IP: $f(n) = 3^n$ a $f(n-1) = 3^{n-1}$. Uvažujme $n+1$.

Je-li $n+1$ liché, pak je n sudé a $f(n+1) = 9f(n-1) \stackrel{IP}{=} 9 \cdot 3^{n-1} = 3^{n+1}$.

Je-li $n+1$ sudé, pak je n liché a $f(n+1) = 3f(n) \stackrel{IP}{=} 3 \cdot 3^n = 3^{n+1}$.

g) $f(n) = \begin{cases} 2^{n/2}, & n \text{ sudé;} \\ 2^{(n-1)/2}, & n \text{ liché.} \end{cases}$ (0) $n = 1$ a $n = 2$ OK. (1) $n \in \mathbb{N}$, IP: $f(k) = \begin{cases} 2^{k/2}, & k \text{ sudé;} \\ 2^{(k-1)/2}, & k \text{ liché} \end{cases}$ pro $k = n-1, n$.

Uvažujme $n+1$.

Je-li $n+1$ sudé, pak je i $n-1$ sudé a $f(n+1) = 2f(n-1) \stackrel{IP}{=} 2 \cdot 2^{(n-1)/2} = 2^{(n+1)/2}$.

Je-li $n+1$ liché, pak je i $n-1$ liché a $f(n+1) = 2f(n-1) \stackrel{IP}{=} 2 \cdot 2^{(n-1-1)/2} = 2^{n/2} = 2^{((n+1)-1)/2}$.

Alternativa: $f(n) = 2^{\lfloor n/2 \rfloor}$.

h) Jak zapsat 1, 0, 2, 2, 0, 4, 4, 0, 8, 8, 0, 16, 16, 0, ...? Nápad: $f(n) = \begin{cases} 0, & n = 3k+1; \\ 2^{\lfloor (n+1)/3 \rfloor}, & n \neq 3k+1. \end{cases}$

Důkaz silnou (modifikovanou) indukcí podobný předchozímu, ale teď se musí řešit tři případy.

7b.7: a) Silná (modifikovaná) indukce (0) Pro $n = 1, 2$ OK. (1) $n \geq 2$, IP: $V(k)$: $f(n) \leq n!$ a $f(n-1) \leq (n-1)!$.

Pak $f(n+1) = f(n) + n f(n-1) \stackrel{IP}{\leq} n! + n \cdot (n-1)! = 2n! \leq (n+1)n! = (n+1)!$.

b) Silná (modifikovaná) indukce (0) Pro $n = 1, 2$ OK. (1) $n \geq 2$, IP: $f(n) \leq n^2$ a $f(n-1) \leq (n-1)^2$. Pak

$f(n+1) = \frac{1}{n}f(n) + f(n-1) \stackrel{IP}{\leq} \frac{1}{n}n^2 + (n-1)^2 = n + n^2 - 2n + 1 = n^2 - n + 1 \leq n^2 + 2n + 1 = (n+1)^2$.

c) Silná (modifikovaná) indukce (0) Pro $n = 1, 2$ OK. (1) $n \geq 2$, IP: $f(n) = n!$ a $f(n-1) = (n-1)!$. Pak

$f(n+1) = n f(n) + n f(n-1) \stackrel{IP}{=} n \cdot n! + n \cdot (n-1)! = n \cdot n! + n! = (n+1) \cdot n! = (n+1)!$.

d) Silná (modifikovaná) indukce (0) Pro $n = 1, 2$ OK. (1) $n \geq 2$, IP: $f(n) \geq n!$ a $f(n-1) \geq (n-1)!$. Pak

$f(n+1) = n f(n) + n^2 f(n-1) \stackrel{IP}{\geq} n \cdot n! + n^2 \cdot (n-1)! = n \cdot n! + n \cdot n! = 2n \cdot n! \geq (n+1) \cdot n! = (n+1)!$.

e) Silná (modifikovaná) indukce (0) Pro $n = 1, 2, 3$ OK. (1) $n \geq 3$, IP: $f(n) \leq 2^n$, $f(n-1) \leq 2^{n-1}$ a $f(n-2) \leq 2^{n-2}$.

Pak $f(n+1) = f(n-2) + f(n-1) + f(n) \stackrel{IP}{\leq} 2^{n-2} + 2^{n-1} + 2^n \leq 2^{n-1} + 2^{n-1} + 2^n = 2 \cdot 2^{n-1} + 2^n = 2^n + 2^n = 2^{n+1}$.

7b.8: A) F_{3k} sudé, F_{3k+1} a F_{3k+2} liché. Důkaz najednou indukcí: (0) $k = 0$ funguje, pokud doplníme $F_0 = 0$. (1) $k \geq 0$, IP: $k \in \mathbb{N}_0$ a F_{3k} sudé, F_{3k+1} a F_{3k+2} liché.

Pak $F_{3(k+1)} = F_{3k+3} = F_{3k+2} + F_{3k+1}$. Protože jsou dle indukčního předpokladu F_{3k+2} a F_{3k+1} liché, je $F_{3(k+1)}$ sudé.

Dále $F_{3(k+1)+1} = F_{3k+4} = F_{3k+3} + F_{3k+2}$. Protože je dle indukčního předpokladu F_{3k+2} liché a již jsme dokázali, že F_{3k+3} je sudé, je $F_{3(k+1)+1}$ liché.

Dále $F_{3(k+1)+2} = F_{3k+5} = F_{3k+4} + F_{3k+3}$. Protože jsme dokázali, že F_{3k+4} je liché a F_{3k+3} je sudé, je $F_{3(k+1)+2}$ liché.

B) a) Slabá indukce: (0) $n = 1$ funguje, $1^2 = 1 \cdot 1$.

(1) Předpoklad: Platí to pro jisté $n \in \mathbb{N}$. Pak

$$F_1^2 + F_2^2 + \dots + F_{n+1}^2 = [F_1^2 + F_2^2 + \dots + F_n^2] + F_{n+1}^2 = F_n F_{n+1} + F_{n+1}^2 = F_{n+1}(F_n + F_{n+1}) = F_{n+1} F_{n+2}.$$

Zbytek podobně.

7b.9: Silná indukce. (0) $n = 1$: $1 = 2^0 \cdot 1$.

(1) $n \geq 1$, IP: Všechna přirozená čísla mezi 1 a n včetně lze zapsat jako $2^m \cdot l$, kde $m \in \mathbb{N}_0$ a l liché. A co $n + 1$?
Případ 1: $n + 1$ liché, pak $n + 1 = 2^0(n + 1)$, $0 \in \mathbb{N}_0$.

Případ 3: $n + 1$ sudé, pak $n + 1 = 2k$, $k \in \mathbb{Z}$. Protože $n + 1 \geq 2$, je $k \geq 1$, také $k \leq n$, proto dle IP: $k = 2^l$. Pak $n + 1 = 2^{m+1}l$, kde l liché a $m + 1 \in \mathbb{N}_0$.

7b.10: Silná indukce. (0) $n = 3$: Trojúhelník má součet úhlů $\pi = (3 - 2)\pi$, souhlasí.

(1) $n \geq 3$: IP: Všechny k -úhelníky pro $3 \leq k \leq n$ to splňují. Uvažujme $N = n + 1$. Pak $N \geq 4$. Rozdělíme daný N -úhelník na dva, jeden bude a -úhelník a druhý b -úhelník. Snadno nahlédneme, že $a + b = N + 2$. Máme $a, b \geq 3$, proto $a, b \leq n$. Podle IP jsou jejich součty úhlů $(a - 2)\pi$ a $(b - 2)\pi$. Součet úhlů původního N -úhelníka je součtem těch dvou součtů, tedy $(a - 2)\pi + (b - 2)\pi = (a + b - 4)\pi = (N - 2)\pi = ((n + 1) - 2)\pi$.

7c. Strukturální indukce

Příklad 7c.a: Uvažujme funkci definovanou takto:

$$(0) f(0) = 0, f(1) = \frac{1}{2};$$

$$(1) f(n + 1) = f(n - 1) + 1 \text{ pro } n \geq 1.$$

Díky předchozí sekci už víme, že tak vznikla funkce na \mathbb{N}_0 a také umíme dokázat modifikovanou indukci, že tato funkce splňuje vzorec $f(n) = \frac{1}{2}n$.

Co se stane, když v základním kroku jednu hodnotu vynecháme? Uvažujme tuto funkci:

$$(0_D) g(0) = 0;$$

$$(1_D) g(n + 1) = g(n - 1) + 1 \text{ pro } n \geq 1.$$

Z pohledu klasické indukce je to chyba, ale nevzdávejme to.

Máme $g(0)$. To nám umožní použít vzorec (1_D) s volbou $n - 1 = 0$ neboli $n = 1$ a dostaneme $g(2) = g(0) + 1 = 1$.
Since neumíme získat $g(1)$, protože $g(1) = g(-1) + 1$ nejde, a tím ani $g(3)$ atd., ale nenechme se tím zastavit.
Pomocí $g(2)$ získáme volbou $n = 3$ hodnotu $g(4)$ a postupujeme dál:

$$g(0) \stackrel{(0_D)}{=} 0,$$

$$g(2) \stackrel{(1_D)}{=}_{n=1} g(0) + 1 = 1,$$

$$g(4) \stackrel{(1_D)}{=}_{n=3} g(2) + 1 = 2,$$

$$g(6) \stackrel{(1_D)}{=}_{n=5} g(4) + 1 = 3,$$

$$g(8) \stackrel{(1_D)}{=}_{n=7} g(6) + 1 = 4, \text{ atd.}$$

Intuice nám říká, že tato induktivní či rekurzivní definice vytvořila funkci g na množině všech nezáporných sudých čísel, označme ji pracovně S . Třeba bychom také tipli, že $g(n) = \frac{1}{2}n$ pro $n \in S$.

V tom okamžiku bychom mohli prohlásit, že nešlo o chybu, ale záměr. Máme novou podobu indukce.

Všimli jsme si, že nedokážeme využít předpis $g(3) = g(1) + 1$, který nám induktivní vzorec také nabízí, vlastně jej nedokážeme využít pro žádné sudé n . Stačil by tedy zápis

$$(1_D) g(n + 1) = g(n - 1) + 1 \text{ pro } n \geq 1, n \text{ liché,}$$

popřípadě elegantní varianta

$$(1_D) g(n + 2) = g(n) + 1 \text{ pro } n \geq 0, n \text{ sudé.}$$

Ta je u pokročilejší indukce populárnější, ze známého n se přejde k nějakému novému, které nemusí být $n + 1$.

Nicméně u nového typu indukce, který zde představujeme, nebývá zvykem indukční vzorec omezovat jinak než podmínkou $n \geq n_0$. Jak dále uvidíme, předpokládá se, že pokud pro některé n nemáme vstupní data, tak se prostě příslušný vzorec nepoužije.

Předchozí zkušenost naznačuje, že rovnost $g(n) = \frac{1}{2}n$ by mělo jít dokázat indukcí, která bude mít stejnou strukturu jako definice funkce g , tedy základní krok s jednou hodnotou a indukční krok skákající o dvě. Z estetických důvodů použijeme tu poslední variantu kroku (1_D).

(0) $n = 0$: $g(0) \stackrel{(0_D)}{=} 0 = \frac{1}{2} \cdot 0$, souhlasí.

(1) Dáno $n \geq 0$ sudé. IP: $g(n) = \frac{1}{2}n$. Pak

$$g(n+2) \stackrel{(1_D)}{=} g(n) + 1 \stackrel{IP}{=} \frac{1}{2}n + 1 = \frac{1}{2}(n+2).$$

□

△

Platnost tohoto důkazu je založena na možnosti projít množinou S pomocí schématu

$$(0) n = 0; \quad (1) n \implies (n+2) \text{ pro } n \geq 0.$$

V poznámce 7b.3 jsme upozornili na existenci dvou vrstev indukce. V prvních dvou sekcích jsme se soustředili na to, abychom správně zvolili schéma pro daný problém a pak jej korektně aplikovali. V této sekci se zaměříme na první vrstvu, tedy na to, jak pomocí zvoleného schématu ovlivnit množinu, na které pracujeme.

U klasické indukce bylo základním požadavkem, abychom schématem vytvořili množinu \mathbb{N} nebo její vhodný posun. Například slabá indukce používá schéma

$$(0) n = 1; \quad (1) n \implies (n+1) \text{ pro } n \geq 1,$$

kteřé projde všemi přirozenými čísly. Jak to víme? Na to potřebujeme vědět, co jsou to vlastně přirozená čísla. Jednou z možných odpovědí je, že je to právě množina vzniklá tímto schématem.

Příklad 7c.b: Peano definoval přirozená čísla takto:

(0) 1 je přirozené číslo;

(1) Pokud je n přirozené číslo, tak $n+1$ je přirozené číslo.

V indukčním kroku chybí rozsah pro n , protože zde představíme nový koncept, používaný u obecných indukcí: Krok je možné použít kdykoliv a kolikrát se nám zachce, pokud umíme splnit předpoklad. Jak to funguje?

Díky kroku (0) víme, že $n = 1$ je přirozené číslo, tudíž je možné použít (1) s $n = 1$ a zjistíme, že 2 je přirozené číslo. To nám umožní použít (1) s dvojkou a zjistíme, že 3 je přirozené číslo. Atd.

Pokud přijmeme Peanovu definici přirozených čísel, pak schéma ze slabé indukce opravdu prochází množinou, kterou chceme.

Podotkněme, že je rozdíl mezi definicí množiny obecným indukčním schématem, které zavedeme v této kapitole, a důkazem klasickou indukcí (slabá, silná, modifikovaná atd.). V definici teď rozsah pro krok (1) neuvádíme, protože uživatel induktivní vzorec používá dle libosti a tím vznikne nějaká množina M použitelných čísel n .

U klasického důkazu indukcí ovšem potřebujeme, aby se tou množinou M stalo \mathbb{N}_0 či nějaký její posun, což je zaručeno správnou návazností kroků indukce. Jinak řečeno, v situacích řešených v předchozích dvou sekcích ty rozsahy pro krok (1) psát opravdu musíme.

△

Hlavním tématem této sekce je možnost vytvářet standardní i zajímavé množiny pomocí indukčních schémat. Induktivní definice množiny má dvě základní složky:

- V základním kroku zasadíme „semínka“ neboli specifikujeme konkrétní objekty, které ve vytvářené množině chceme.
- Do induktivní části zařadíme jedno či více pravidel, která pomocí již existujících objektů (jednoho či více) vytvoří nový objekt.

Formálně:

Induktivní definice množin.

Induktivní definice množiny M se skládá z následujících částí:

(0) **Základní pravidla** definují přímo, které prvky jsou v množině M .

(1) **Indukční pravidla** určují, jak lze pomocí prvků, které již v množině jsou (tzv. **předpoklady** pravidla), vytvářet další prvky z M (tzv. **závěr** pravidla).

Množina M se pak skládá ze všech prvků, které lze obdržet konečným počtem použití pravidel (0) a (1) (tedy prvky, které lze takto získat, leží v M , a ty, které takto získat nelze, pak v M neleží, čímž je množina M jednoznačně určena).

V definici hraje významnou roli vymezení, že prvky vznikají jen konečným počtem aplikací pravidel. Existuje širší teorie, která toto omezení nemá. Pak nám Peanova definice po nekonečném počtu opakování kroku (1) vyrobí nekonečno jako objekt, čímž to začne být zajímavé. (Co je to? A co dostaneme, když k tomu indukčním krokem ještě přičteme jedničku?) O této „transfinitní indukci“ zde určitě nebudeme mluvit, spokojíme se s konečným (ale libovolně velkým) používáním pravidel při vytváření prvků.

Když takovým schématem vytvoříme množinu, tak na ní můžeme zadefinovat nějaký objekt, popřípadě na této množině dokázat nějakou vlastnost. Důkaz pak musí mít stejnou strukturu jako definice.

7c.1. Princip strukturální indukce (structural induction).

Uvažujme množinu M definovanou induktivně pomocí nějakých základních pravidel (0_D) a indukčních pravidel (1_D). Uvažujme vlastnost $V(m)$, která má smysl pro všechna $m \in M$.

Předpokládejme, že

(0) V platí pro všechny prvky, které jsou do M dodány základními pravidly.

(1) Pro každé indukční pravidlo je pravdivá následující implikace: Jestliže V platí pro prvky z jeho předpokladů, pak platí také pro prvek z jeho závěru.

Pak vlastnost V platí pro všechny prvky $m \in M$.

Příklad 7c.c: Uvažujme množinu M definovanou takto:

(0a) $9 \in M$,

(0b) $15 \in M$;

(1a) $m, n \in M \implies m + n \in M$,

(1b) $m, n \in M \implies m - n \in M$.

Tento způsob zadání pravidel je vhodný pro situace, kdy se na ně budeme chtít odvolávat. Jinak je běžná stručnější podoba, třeba

(0) $9 \in M, 15 \in M$;

(1) $m, n \in M \implies m \pm n \in M$.

Co je to za množinu? Než to zjistíme, zkusíme o ní něco dokázat. Například si všimneme, že základní hodnoty jsou obě dělitelné třemi a sčítání či odčítání to nemůže pokazit. To je jádro důkazu strukturální indukci, že každé číslo v M je dělitelné třemi. Formálně:

(0) V základním kroku do množiny přidáváme čísla 9 a 15, která jsou obě dělitelná třemi.

(1) Pravidlo (1a): Jestliže jsou čísla m, n dělitelná třemi (prvky předpokladu splňují tvrzení), pak je dělitelné třemi i číslo $m + n$ (prvek se závěru splňuje tvrzení). Použili jsme fakt 1a.17.

Pravidlo (1b): Jestliže jsou čísla m, n dělitelná třemi, pak je dělitelné třemi i číslo $m - n$.

□

Vlastně jsme ukázali, že

$$M \subseteq \{3k; k \in \mathbb{Z}\}.$$

Experimentování s pravidly nás může přivést k pocitu, že pomocí nich dokážeme vytvořit všechny násobky tří, tedy že vlastně máme množinovou rovnost a známe přesnou identitu množiny M . Jednu inkluzi máme, potřebujeme tu opačnou. To dokážeme ve třech krocích.

V přípravném kroku ukážeme, že $3 \in M$. Volbou $m = 15, n = 9$ (jsou v M podle základního kroku) zjistíme, že podle (1b) také $15 - 9 = 6 \in M$. Pak máme právo aplikovat (1b) s volbou $m = 9, n = 6$ a potvrdíme, že $3 \in M$.

Nyní klasickou indukci dokážeme, že $\{3k; k \in \mathbb{N}_0\} \subseteq M$.

(0) $k = 0$: Protože $3 \in M$, podle pravidla (1b) je i $3 - 3 = 0 = 3 \cdot 0 \in M$.

(1) $k \geq 0$, IP: $3k \in M$. Také $3 \in M$, proto podle (1a) leží v M i $3k + 3 = 3(k + 1)$.

□

Zbývá ukázat $\{-3k; k \in \mathbb{N}_0\} \subseteq M$, což čtenář snadno udělá úpravou předchozího důkazu.

△

M Tento příklad je netypický v tom, že jsme vytvořili definici a pak zjišťovali, co vlastně vzniklo. Obvykle je to naopak: Máme přesnou představu, jakou množinu N chceme vytvořit, typicky jsou to objekty s jistou vlastností. Zkusíme vymyslet základní a indukční pravidla, která by ji vytvořila, ale to je třeba potvrdit. Zatím víme jen to, že naše pravidla vytvářejí nějakou množinu M . Rovnost $M = N$ se obvykle ověřuje ve dvou krocích, podobně jako v předchozím příkladě.

Snadnější bývá inkluze $M \subseteq N$, kdy dokazujeme, že všechny objekty vytvořené pomocí našich pravidel mají žádanou vlastnost. K tomu slouží strukturální indukce.

Opačná inkluze $N \subseteq M$ znamená potvrdit, že se k libovolnému objektu z N dokážeme dostat pomocí našich indukčních pravidel. To se často dělá vhodnou indukcí (slabou, silnou) například podle žádané vlastnosti.

Příklad 7c.d: Vytvoříme induktivní definici množiny $M_{2(5)}$ přirozených čísel, jejichž zbytek po dělení pěti je 2. Když si rozmyslíme, jak tato čísla vypadají, popřípadě když se zamyslíme, jak z většího čísla s touto vlastností vytvořit menší a naopak, dospějeme k této specifikaci:

(0_D) $2 \in M$;

(1_D) Jestliže $n \in M$, pak $n + 5 \in M$.

Tím vznikla množina M jistých objektů. Dokážeme, že je rovna žádané množině $M_{2(5)}$.

1. Nejprve ukážeme, že $M \subseteq M_{2(5)}$, tedy že objekty vytvořené naší definicí jsou všechno přirozená čísla se zbytkem po dělení rovným 2. Jde o vlastnost prvků množiny M , tedy použijeme princip strukturální indukce.

(0) V základním kroku jsme do množiny vložili $n = 2$. To je přirozené číslo a $2 \bmod 5 = 2$, tedy $2 \in M_{2(5)}$.

(1) Uvažujme nějaký předpoklad pravidla (1_D) , tedy prvek $n \in M$ a předpokládejme, že $n \in M_{2(5)}$. Je to tedy přirozené číslo a $n \bmod 5 = 2$. Závěr pravidla pak přidá do M číslo $n + 5$, které je zjevně celé a díky $n + 5 \geq n \geq 1$ také přirozené. Protože $n + 5 \equiv n \pmod{5}$, musí podle věty 2a.1 platit

$$n + 5 \bmod 5 = n \bmod 5 = 2,$$

tedy $n + 5 \in M_{2(5)}$. Ukázali jsme, že dokazovaná vlastnost se přenáší z předpokladu pravidla na jeho závěr.

□

2. Nyní ukážeme, že $M_{2(5)} \subseteq M$, tedy že každé přirozené číslo se zbytkem 2 při dělení pěti lze získat aplikováním pravidel z (0_D) a (1_D) . Tato část důkazu může být velmi obtížná a obvykle pomůže, pokud žádaná čísla dokážeme nějak popsát. V tomto případě díky kapitole 1 víme, že množinu $M_{2(5)}$ lze zapsat jako

$$M_{2(5)} = \{5k + 2; k \in \mathbb{N}_0\}.$$

Ukážeme indukcí, že všechna čísla tohoto typu lze vytvořit pravidly. V tomto případě pracujeme s $k \in \mathbb{N}_0$, tedy použijeme běžnou slabou indukcí.

(0) $k = 0$: Číslo $5 \cdot 0 + 2 = 2$ umíme získat pomocí pravidla (0_D) , tedy $2 \in M$.

(1) Dáno $k \geq 0$. Předpokládejme, že $5k + 2 \in M$, tedy číslo $5k + 2$ lze vytvořit nějakou konkrétní aplikací základních a indukčních pravidel (0_D) a (1_D) . Když toto ještě následujeme jednou aplikací pravidla (1_D) , tak vznikne číslo $5k + 2 + 5 = 5(k + 1) + 2$, které jsme tedy dokázali vytvořit aplikací pravidel z (0_D) a (1_D) a proto $5(k + 1) + 2 \in M$.

□

△

Dokázat, že naše pravidla dávají přesně žádanou množinu, nemusí být snadné a ne vždy to zde budeme dělat. Hlavním cílem je strukturální indukci porozumět a naučit se takové definice vytvářet. Ale vyplatí se alespoň zamyslet, zda se opravdu definicí dostaneme ke všem potřebným prvkům.

Naši přehlídku nápadů začneme otázkou, jak vytvářet standardní množiny.

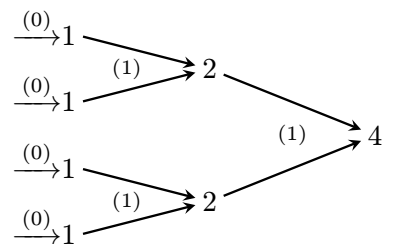
Příklad 7c.e: Viděli jsme Peanovu definici \mathbb{N} založenou na schématu slabé indukce, obdobně bychom mohli definovat \mathbb{N} pomocí schématu silné indukce. Jsou ale další alternativy, například tato:

(0) 1 je přirozené číslo.

(1) Pokud jsou m, n přirozená čísla, tak je také $m + n$ přirozené číslo.

Opravdu? Formálně, v podmínce (1) je vždy možné volit $m = 1$, takže tato definice v sobě zahrnuje tu Peanovu. Zároveň si rozmyslíme, že ve skutečnosti nepřidává nic navíc.

Oproti Peanově definici se liší tím, že plýtvá. Zatímco k číslu 2 se Peano i tato definice dostanou stejně, ke čtyřce už se novou definicí umíme dostat více způsoby. Kromě toho Peanova $1 \xrightarrow{+1} 2 \xrightarrow{+1} 3 \xrightarrow{+1} 4$ lze také použít odvození napravo.



Peanův přístup je tedy efektivnější.

△

7c.2 Poznámka:

Když máme množinu M definovanou indukcí, tak se každý prvek z M vytvořil nějakým konečným počtem použití pravidel z (0) a (1). V aplikacích bývá užitečné zjistit, jak to proběhlo.

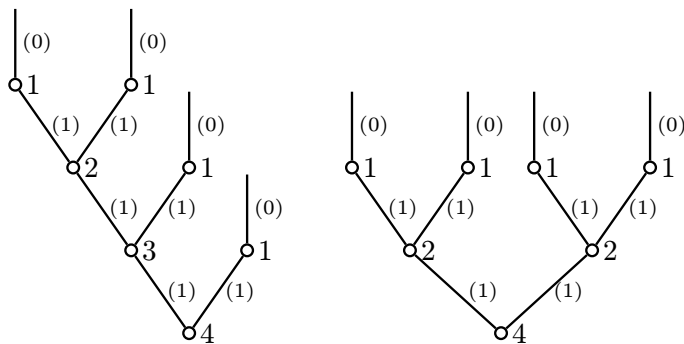
Říká se tomu derivační postup a existují různé textové i grafické formáty pro jeho zachycení. Názorný je **derivační strom** či **odvozovací strom** (anglicky **parsing tree**). Populární verze nákrese má prvek dole jako kořen. Pomocí hran se ukáže, pomocí jakých prvků se k němu přišlo, přičemž příslušné pravidlo se píše ke hranám jako poznámka. Od prvků se jde vzhůru k jejich předchůdcům, dokud se nedorazí k listům, tj. prvkům ze základních pravidel (0).



Vpravo vidíme odvození čtyřky podle pravidel z Peanovy definice přirozených čísel.

Počet úrovní stromu (přesněji řečeno největší počet kroků, který je ve stromu možné jedním směrem udělat) je **výška** stromu, ta pak určuje **výšku prvku**. Takže prvky ze základních pravidel mají výšku 1 (nejprve je nic, jedním krokem dle pravidla (0) se pak dojde k dotyčnému prvku). Vidíme, že v přirozených číslech podle Peana má čtyřka výšku 4.

V alternativní definici s pravidlem $m + n$ se lze ke čtyřce dostat více způsoby, dva možné vidíme níže.



V případě, že je odvozovacích stromů více, se výška prvku určuje podle nejnižšího stromu. Pokud dokážeme, že nižší strom než ten napravo pro čtyřku neexistuje, tak bude její výška v alternativních přirozených číslech rovna $\min(4, 3) = 3$.

Vidíme, že definice, které umožňují vznik prvků více způsoby, v sobě zahrnují určité komplikace.

△

Protože tento formát odvozovacích stromů je náročný na prostor, budeme v jednodušších případech využívat alternativní zápis (doufejme stejně srozumitelný).

Příklad 7c.f: Jak vytvoříme indukci celá čísla? Ta utíkají do nekonečna dvěma směry, takže přirozený způsob je použít dvě indukční pravidla.

- (0) 0 je celé číslo.
- (1a) Jestliže je n celé číslo, tak je také $n + 1$ celé číslo.
- (1b) Jestliže je n celé číslo, tak je také $n - 1$ celé číslo.

Tato definice opět plýtvá, například k číslu 1 se dokážeme dostat nekonečně mnoha způsoby, třeba těmito dvěma:

$$\xrightarrow{(0)} 0 \xrightarrow{(1a)} 1, \quad \xrightarrow{(0)} 0 \xrightarrow{(1b)} -1 \xrightarrow{(1a)} 0 \xrightarrow{(1a)} 1.$$

Pokud nepotřebujeme rozlišovat mezi pravidly, tak je možné indukční krok napsat jako

- (1) Jestliže je n celé číslo, tak jsou také $n - 1$ a $n + 1$ celá čísla.

Existuje zajímavá možnost definovat celá čísla jediným indukčním krokem:

- (0) 1 je celé číslo.
- (1) Jestliže jsou m, n celá čísla, tak je také $m - n$ celé číslo.

Když aplikujeme (1) s volbou $m = n = 1$, dozvíme se, že 0 je celé číslo. Opakovaným použitím (1) s $n = 1$ dostaneme krok $m \mapsto m - 1$, kterým od startovací hodnoty $m = 0$ vytvoříme záporná celá čísla, například -1 pomocí $m = 0, n = 1$. Volbou $n = -1$ pak zjistíme, že když je m celé, tak je i $m + 1$ celé, čímž se dostaneme ke kladným celým číslům.

Mít jen jedno indukční pravidlo je elegantní, nicméně i tato definice umožňuje získat jedno číslo více způsoby. Efektivní zavedení celých čísel, tedy s jednoznačným odvozovacím stromem pro prvky, nejspíše neexistuje.

△

Příklad 7c.g: Zajímavou výzvou jsou prostory více dimenzí, například \mathbb{N}^2 . Ty je možné vytvářet více způsoby, populární je tento.

- (0) $(1, 1) \in M$;
- (1) $(1, n) \in M \implies (1, n + 1) \in M$,
- $(m, n) \in M \implies (m + 1, n) \in M$.

Intuitivně to funguje: Pokud se chceme dostat do nějaké lokace (x, y) , tak nejprve pomocí prvního indukčního pravidla dorazíme do lokace $(1, y)$ a pak pomocí druhého do (x, y) .

Je samozřejmě možné použít alternativu, kdy první pravidlo pracuje s první souřadnicí a druhá je rovna jedné, načež se v druhém pravidle posune druhá souřadnice.

Problém je, že když se pomocí takového schématu pokoušíme něco dokázat, tak ta vlastnost musí dobře spolupracovat právě s tímto schématem, jinak důkaz neprojde, ačkoliv je schéma správné. Ale třeba projde jiné. Nebo ta vlastnost indukci dokázat nejde vůbec.

Podobný problém máme při dokazování vlastností pro racionální čísla. Není problém vyrobit schéma, které obsáhne všechny zlomky, například toto:

$$(0) \frac{0}{1} \in M;$$

$$(1) \frac{p}{q} \in M \implies \frac{p}{q+1} \in M, \frac{p+1}{q} \in M, \frac{p-1}{q} \in M.$$

Není těžké ukázat, že $M = \mathbb{Q}$. Ovšem těžko budeme hledat nějakou užitečnou vlastnost racionálních čísel, která by byla v souladu s tímto schématem a umožnila tak důkaz indukci.

△

Modifikací základních schémat můžeme vybírat ze známých množin. Již jsme viděli schéma pro sudá čísla, které hravě upravíme pro lichá čísla. Viděli jsme i obecnější případ kongruenčních tříd. Snadno nahlédneme, že

$$(0) 1 \in M; \quad (1) n \in M \implies a \cdot n \in M$$

vytvoří množinu $M = \{a^k; k \in \mathbb{N}_0\}$ nezáporných mocnin čísla a .

Všechny tyto množiny umíme vytvořit elegantním vzorcem, viz tato množina mocnin. Není tedy jasné, co nám přináší induktivní definice. Odpověď zní, že pro některé vlastnosti jsou tradiční nástroje vhodné, ale jsou také vlastnosti, které se jimi zvládají obtížně. Ukažme jednu z klíčových aplikací, která navíc zavede užitečný jazyk.

! Příklad 7c.h: V takzvané teorii jazyků je výchozím objektem „abeceda“, což je libovolná množina Σ objektů, ze kterých hodláme vytvářet řetězce. Mohla by to být množina malých písmen anglické abecedy, nebo třeba množina cifer. Typicky se jim říká znaky.

Slepováním znaků za sebe vznikají řetězce. Slepovat se dají i řetězce za sebe, jeden znak je vlastně také řetězec. V teorii jazyků se této operaci říká konkatenace a pro řetězce α, β se značí $\alpha\beta$. Pokud nás například zajímá případ s anglickou abecedou, tak pro řetězce $\alpha =$ „auto“ a $\beta =$ „mat“ je výsledkem jejich konkatenace řetězec $\alpha\beta =$ „automat“. Je evidentní, že tato operace není komutativní.

Hlavním objektem v teorii jazyků je množina všech řetězců Σ^* , kterým se v této teorii říká „slova“, čímž se ovšem nenutí, aby měla nějaký význam. Například „xqwyř“ je legitimní „slovo“ nad běžnou abecedou. Jedno zajímavé slovo je prázdné značené λ , které se skládá z žádných znaků.

Množina Σ^* všech slov nad abecedou Σ se standardně definuje induktivně pomocí konkatenace:

$$(0) \lambda \in \Sigma^*;$$

$$(1) \text{ Jestliže } w \in \Sigma^* \text{ a } c \in \Sigma, \text{ pak } wc \in \Sigma^*.$$

Tato definice odpovídá běžné praxi, kdy píšeme písmeno po písmenu zleva doprava.

Podotkneme, že jsme zase zapsali (1) ve zkrácené formě, což se dělá běžně, ale není to zcela formálně správně. Indukční pravidla totiž mohou mít na vstupu jen již existující objekty, což je to slovo w . Správně bychom měli pro každý prvek c z abecedy Σ vytvořit speciální indukční pravidlo, které jej přilepí zprava k existujícímu řetězci. Uvidíme to v příkladě 7c.k.

V některých aplikacích je potřeba se prázdnému řetězci vyhnout, pak bychom pracovali s množinou danou předpisem

$$(0) c \in \Sigma^* \text{ pro } c \in \Sigma;$$

$$(1) \text{ Jestliže } w \in \Sigma^* \text{ a } c \in \Sigma, \text{ pak } wc \in \Sigma^*.$$

Tentokrát jsme použili zkrácený zápis také v základním kroku, kde je ve skutečnosti schováno mnoho pravidel; pro každý objekt c z abecedy je tam speciální pravidlo, které jej zařadí do Σ^* . Často se to zapisuje takto:

$$(0) c \in \Sigma \implies c \in \Sigma^*.$$

Od induktivní části (1) se to liší v tom, že indukční pravidla pracují s již existujícími prvky ze Σ^* a modifikují je, tedy jde o indukci, zatímco v kroku (0) forma implikace říká, které konkrétní prvky přímo vkládáme do M . Skutečný význam je $\forall c \in \Sigma: c \in \Sigma^*$.

Užitečnost teorie jazyků spočívá v tom, že úpravou indukčních pravidel je možné vybírat jen taková slova, která vyhovují určitým pravidlům, čímž se do jazyka zanesou gramatika.

△

Příklad 7c.i: Chceme induktivně zadefinovat množinu všech slov nad anglickou abecedou, které tvoří palindromy, tedy čtou se stejně v obou směrech. Připomeňme, že jde o slova matematická, tedy nemusejí dávat smysl, proto kromě klasik jako „radar“ nebo „nepotopen“ bereme i „abcba“. Intuitivně se to zdá jasné: Začneme uprostřed a budeme k oběma krajům připisovat totéž. Pro usnadnění značení si zavedeme množinu C všech povolených písmen. Protože w je teď legitimní písmeno (prvek abecedy), budeme pro slova používat řeckou omegu.

První pokus:

$$(0) c \in C \implies c \in M;$$

$$(1) \omega \in M, c \in C \implies c\omega c \in M.$$

Takto dostaneme třeba ten „radar“, ale všímavého čtenáře napadne, že těmito pravidly lze vytvářet pouze palindromy s lichým počtem znaků, takže se neumíme dostat třeba k palindromu „anna“. Lepší pokus:

$$(0) c \in C \implies c \in M, cc \in M;$$

$$(1) \omega \in M, c \in C \implies c\omega c \in M.$$

Tohle už funguje.

Opět se nám nechtělo psát pravidla formálně správně. Měli bychom totiž mít 26 pravidel základních

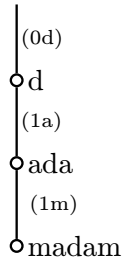
$$(0a) a \in M, (0b) b \in M, \dots, (0z) z \in M;$$

a 26 pravidel indukčních:

$$(1a) \omega \in M \implies a\omega a \in M, (1b) \omega \in M \implies b\omega b \in M, \dots, (1z) \omega \in M \implies z\omega z \in M.$$

Pak se na ně můžeme odvolávat například v odvozovacím stromě pro „madam“.

U této definice vzniká každý palindrom unikátním způsobem, je tedy efektivní a uživatelsky příjemnější.



△

Pokud chceme s řetězci něco dělat či o nich něco zjišťovat, je indukce přirozeným nástrojem.

Příklad 7c.j: Předpokládejme, že máme abecedu Σ a množinu slov definovanou jako

$$(0) \lambda \in \Sigma^*;$$

$$(1) w \in \Sigma^*, c \in \Sigma \implies wc \in \Sigma.$$

Pak můžeme definovat funkci délku slova w , značenou $l(w)$, jako

$$(0) l(\lambda) = 0;$$

$$(1) w \in \Sigma^*, c \in \Sigma \implies l(wc) = l(w) + 1.$$

Jak je dlouhý třeba řetězec „bat“ nad anglickou abecedou?

Podle definice vzniklo „bat“ připojením posledního znaku zprava, tedy jako „(ba)t“, a tudíž podle druhé definice máme $l(bat) = l(ba) + 1$. Stejně si rozmyslíme, jak to pokračuje:

$$l(bat) = l(ba) + 1 = (l(b) + 1) + 1 = ((l(\lambda) + 1) + 1) + 1 = ((0 + 1) + 1) + 1 = 3.$$

Asi nás to nepřekvapilo.

△

Nyní na jednom užitečném případě porovnáme výhody a nevýhody explicitního versus induktivního přístupu.

Příklad 7c.k: Populárním objektem ve světě počítačů jsou binární řetězce neboli útvary typu 100110111. Lze je vnímat jako čísla vyjádřená v binární soustavě, tedy výchozí množinou by bylo \mathbb{N} . Pokud chceme pracovat s jednotlivými ciframi, pak se nabízí přepis $n = \sum_{k=0}^N c_k 2^k$ pro nějaká $c_k \in \{0, 1\}$. My s nimi ale nechceme počítat, takže bude zajímavější zápis řetězců coby vektorů cifer,

$$M_1 = \{(c_0, \dots, c_N); N \in \mathbb{N}_0, c_k \in \{0, 1\} \text{ pro } k \in \{0, 1, \dots, N\}\}.$$

Zajímavou alternativou je vnímat binární řetězce jako slova nad abecedou $\Sigma = \{0, 1\}$. Protože v počítačích prázdný řetězec nemá jako číslo smysl, použijeme definici, která jej nedovoluje. V této definici 0 a 1 nepředstavují čísla, ale znaky. Protože jde o alternativní pohled, budeme množině říkat M_2 :

$$(0) 0 \in M_2, 1 \in M_2.$$

$$(1) w \in M_2, c \in \{0, 1\} \implies wc \in M_2.$$

Opět jde o zkrácený zápis, ve skutečnosti máme čtyři specifikace:

$$(0a) 0 \in M_2,$$

$$(0a) 1 \in M_2;$$

$$(1a) w \in M_2 \implies w0 \in M_2,$$

$$(1b) w \in M_2 \implies w1 \in M_2.$$

Tato definice odpovídá tomu, jak bychom rukou napsali binární řetězec. Začneme cifrou a k ní připojujeme další. Mohli bychom ovšem řetězce psát i zprava doleva, takže máme alternativní definici:

$$(0) 0 \in M_2, 1 \in M_2;$$

$$(1) w \in M_2, c \in \{0, 1\} \implies cw \in M_2.$$

Dokonce můžeme uživateli umožnit připojovat cifry k existujícímu řetězci zleva i zprava. Sice budeme plýtvat (stejný řetězec lze získat více způsoby), ale je to legitimní volba.

$$(0) 0 \in M_2, 1 \in M_2;$$

- (1) $w \in M_2, c \in \{0, 1\} \implies wc \in M_2,$
 $w \in M_2, c \in \{0, 1\} \implies cw \in M_2.$

Zde vlastně induktivní část obsahuje čtyři pravidla, protože bychom správně měli mít speciální pravidla umožňující přidání znaku 0 zprava, 1 zprava, 0 zleva, 1 zleva.

Pro úplnost ještě ukažme další plýtvavou definici:

- (0) $0 \in M_2, 1 \in M_2;$
 (1) $w_1, w_2 \in M_2 \implies w_1w_2 \in M_2.$

Zde jsou na vstupu dva již existující objekty, což je formálně v pořádku a je to jedno existující pravidlo, nikoliv populární zkratka pro více pravidel.

Zajímavý nápad je tento:

- (0) $1 \in M_3, 0 \in M_3.$
 (1) $w \in M_2, c_1, c_2 \in \{0, 1\} \implies c_1wc_2 \in M_3.$

Tím také vznikne množina binárních řetězců, ale ne všech. Indukční pravidlo nás nutí přidat znak před a za řetězec, takže nikdy nedokážeme vytvořit řetězec se sudým počtem znaků, třeba 11. Není to tedy správná definice.

Nyní budeme na řetězce klást rozličné požadavky a uvidíme, jak si s nimi ty dva přístupy, algebraický a jazykový, poradí.

- 1.** Chceme binární řetězce s jedničkou na pravém konci.

Algebraický přístup:

$$M = \{(c_0, \dots, c_N); N \in \mathbb{N}_0, c_k \in \{0, 1\} \text{ pro } k \in \{0, \dots, N-1\}, c_N = 1\}.$$

Induktivní přístup: Je to snadné, začneme jedničkou a k ní lepíme znaky zleva.

- (0) $1 \in M;$
 (1) $w \in M, c \in \{0, 1\} \implies cw \in M.$

- 2.** Chceme binární řetězce, aby na třetím místě zleva byla jednička.

Algebraický přístup:

$$M = \{(c_0, \dots, c_N); N \in \mathbb{N}_0, N \geq 2, c_k \in \{0, 1\} \text{ pro } k \in \{0, \dots, N\}, c_2 = 1\}.$$

Induktivní přístup: Nemůžeme v základním kroku zasadit jedničku a pak dovolit uživateli, aby k ní lepil zleva a zprava. Podstatou induktivní definice je, že při vytváření objektů lze pravidla z (1_D) používat, kolikrát se nám chce, takže jakmile dovolíme přidat znak zleva, tak nelze donutit uživatele, aby toto pravidlo použil přesně dvakrát. Dá se to zachránit fintou, že v základním kroku přidáme všechny možné levé začátky.

- (0) $001 \in M, 011 \in M, 101 \in M, 111 \in M;$
 (1) $w \in M, c \in \{0, 1\} \implies wc \in M.$

Pokud bychom chtěli řetězce, kde je na šestém místě zleva jednička, tak bychom se u induktivní definice v kroku (0) dost zapotili (2^5 možností), tady je algebraický přístup zjevně lepší.

- 3.** Chceme binární řetězce, ve kterých se jedničky vyskytují ve skupinách se sudým počtem po sobě jdoucích jedniček. Takže 110111000011 je v pořádku, ale 1110 ne.

Algebraický přístup zde nenabízí rozumnou cestu. Induktivní přístup je naopak velmi efektivní, protože prostě dovolíme tvůrci přepisovat k řetězcům jedničky jen po dvojicích.

- (0) $0 \in M, 11 \in M;$
 (1) $w \in M \implies w0 \in M,$
 $w \in M \implies w11 \in M.$

Mohli bychom také dovolit přepisování zleva, popřípadě (neefektivně) z obou stran.

Mimochodem, je zjevné, že tato definice vytváří správné objekty, protože takto není možno vyrobit řetězec, ve kterém by šel po sobě lichý počet jedniček. Ale dokázat, že tímto předpisem dokážeme vytvořit všechny žádané řetězce, už dá trochu práce. Použila by se indukce na délku řetězce.

Krok stranou: Co kdybychom chtěli vědět, kolik daný řetězec obsahuje (nepřekrývajících se) dvojic 11? Zavedli bychom na to funkci $f(w)$.

- (0) $f(0) = 0, f(11) = 1;$
 (1) $w \in M \implies f(w0) = f(w),$
 $w \in M \implies f(w11) = f(w) + 1.$

Pak rekurentním postupem odvodíme například

$$f(01101111) = f(011011) + 1 = f(0110) + 1 + 1 = f(011) + 1 + 1 = f(0) + 1 + 1 + 1 = 0 + 1 + 1 + 1 = 3.$$

- 4.** Chceme binární řetězce, ve kterých se jednička vyskytuje přesně třikrát.

Algebraický přístup: Indexy k , pro které je $c_k = 1$, dáme do množiny a zjistíme, zda má správnou velikost.

$$M = \{(c_0, \dots, c_N); N \in \mathbb{N}_0, c_k \in \{0, 1\} \text{ pro } k \in \{0, \dots, N\}, |\{k; c_k = 1\}| = 3\}.$$

Induktivní přístup: Máme problém. Pokud dovolíme přidávat jedničku v indukčním kroku, tak nedokážeme uživatele donutit, aby jej použil přesně třikrát. Pokud bychom tři jedničky chtěli vnutit v základním kroku, tak bychom tam museli de facto dát po jednom celou množinu a nebylo by žádné indukční pravidlo, což ztrácí smysl. Tohle nepůjde.

Mimochodem, zpět k algebraickému přístupu: Pro binární řetězce existuje trik na zjištění počtu jedniček:

$$M = \{(c_0, \dots, c_N); N \in \mathbb{N}_0, c_k \in \{0, 1\} \text{ pro } k \in \{0, \dots, N\}, \sum c_k = 3\}.$$

Ale už by to nefungoval třeba u čísel v desítkové soustavě, zatímco původní řešení ano.

5. Chceme binární řetězce, ve kterých se nikdy nevyskytují dvě jedničky po sobě.

Algebraický přístup: Museli bychom do definice množiny zakomponovat podmínku $c_k = 1 \implies c_{k+1} = 0$ pro $k < N$, což by šlo, ale bylo by méně praktické než induktivní přístup.

Induktivní přístup: Použitý formát (pro objekty už v množině přidej další objekt) nedovoluje přidat podmínku (pokud řetězec končí nulou, můžeš přilepit jedničku). Musí se na to jinak. Na vyloučení po sobě jdoucích stejných znaků existuje klasický trik: Dovolíme přidat jedničku zprava, ale povinně s nulou před ní. První nástřel:

- (0) $0 \in M, 1 \in M;$
 (1) $w \in M \implies w0 \in M,$
 $w \in M \implies w01 \in M.$

Toto opravdu vyrábí řetězce bez jedniček vedle sebe, ale ne všechny. Neumí totiž vyrobit legitimní řetězec 01. Abychom to napravili, přidáme jej do základního kroku. Šlo by místo toho přidat prázdný řetězec, což by v teorii fungovalo, u počítačových binárních řetězců spíš ne. Takže druhý pokus:

- (0) $0 \in M, 1 \in M, 01 \in M;$
 (1) $w \in M \implies w0 \in M,$
 $w \in M \implies w01 \in M.$

Toto už je správná definice. Jak to víme? Dobrá otázka. Načtneme důkaz modifikovanou indukcí (s dvěma potřebnými daty v indukčním předpokladu) na délku řetězce, že tato definice umí vyrobit všechny povolené binární řetězce.

Řetězce délky 1 jsou 0 a 1, oba povolené, oba v základním kroku.

Řetězce délky dva jsou povoleny tři, 00, 01, 10. První a třetí se získají přidáním nuly ke znaku ze základního kroku, prostřední je v základním kroku.

Pro $n \geq 2$ předpokládejme, že umíme vyrobit všechny povolené řetězce délky n a $n-1$. Mějme libovolný povolený řetězec délky $n+1$. Pokud napravo končí nulou, pak vznikl přidáním nuly k povolenému řetězci délky n , který podle předpokladu umíme vyrobit. Pokud končí jedničkou, pak před ní musí být nula a nějaký řetězec délky $n-1$, který také nesmí mít dvě jedničky za sebou, přičemž $n-1 \geq 1$. Tento řetězec délky $n-1$ umíme vyrobit a přilepením skupiny 01 získáme zkoumaný řetězec. A je to.

△

Příklad 7c.1: Přirozená čísla je možné vnímat také jako řetězce číslic. Potřebujeme na to základní znaky neboli abecedu $C = \{0, 1, 2, \dots, 9\}$ a čísla odpovídají slovům nad touto abecedou. Obvykle je píšeme zleva doprava, čemuž odpovídá tato definice:

- (0) $c \in C \implies c \in M;$
 (1) $w \in M, c \in C \implies wc \in M.$

Pokud bychom nechtěli, aby čísla začínala nulou, upravili bychom základní krok takto:

- (0) $c \in C \setminus \{0\} \implies c \in M;$

Co kdybychom také nechtěli nulu na druhém konci (tedy nechceme čísla dělitelná nulou)? Tak máme problém. Protože nějaké nuly v číslech být mohou, tak musíme dovolit je přidávat v kroku (1), ale induktivní definice neumožňuje zakázat uživateli, aby toto pravidlo nepoužil jako poslední.

Pokud bychom stavěli čísla zprava doleva, tak sice umíme zakázat nulu na pravém konci, ale zase se může objevit na levém.

Co kdybychom povolili přidávat nulu jen s nenulovým znakem za ní? Vypadalo by to nějak takto:

- (1) $w \in M, c \in C \setminus \{0\} \implies w0c \in M.$

Bohužel pak neumíme vytvořit legitimní číslo 1001. Pokud ještě přidáme pravidlo s $w00c$, ta nevytvoříme 10001, atd. Potřebovali bychom nekonečně mnoho pravidel, což nejde.

Zajímavý nápad je dovolit přidávat nulu doprostřed. Ovšem formát pravidel nám neumožní vzít stávající řetězec a rozseknout, takže to budeme muset dělat jinak, spojovat dva existující řetězce s nulou mezi:

- (0) $c \in C \setminus \{0\} \implies c \in M;$
 (1a) $w \in M, c \in C \setminus \{0\} \implies wc \in M.$
 (1b) $v \in M, w \in M \implies v0w \in M.$

Třeba číslo 130742 vyrobíme tak, že pomocí pravidel (0) a (1a) připravíme segmenty 13 a 742 a pak spojíme pomocí (1b). Jenže: Jak vyrobíme 130042? Na to bychom potřebovali pravidlo pro vkládání dvou nul, také tří, čtyř atd. Nekonečně pravidel ovšem použít nemůžeme.

Vidíme, že zakazovat na jednom konci je pro induktivní definici snadné, na obou v zásadě nemožné. Podobně jsme neměli v předchozím příkladě problém vynutit jedničku na levém či pravém konci, ale vynutit ji na obou je indukcí nemožné, zatímco algebraická verze by to zvládla podmínkou $c_0 = 1$, $c_N = 1$.

Poradí si s tím rozšířený formát, která je v některých aplikacích k dispozici. Dovoluje objekty na vstupu strukturovat, v našem případě by se hodilo umět v předpokladu spojovacího pravidla místo $w \in M$ napsat $w_1w_2 \in M$, čímž se myslí jedno existující slovo, které je ale ve chvíli načtení rozříznuto na dvě podslova. Pravidlo ve formě

$$(1) w_1w_2 \in M \implies w_10w_2 \in M$$

už umožní vkládat nulu libovolně dovnitř existujícího slova.

Tento trik také umí elegantně vyřešit další zapeklitý problém. Jak bychom zadefinovali čísla, ve kterých se nevyskytuje třináctka jako podřetězec, tedy 3 není nikdy hned po jedničce? Zaměřme se na problematický indukční krok. Je zjevné, že netrojkové číslice můžeme přilepovat zprava dle libosti. Aby přilepením trojky nevznikla třináctka, budeme muset zároveň dát něco před ní. Nabízí se myšlenka na devět pravidel typu

$$w \in M \implies w03 \in M, \quad w \in M \implies w23 \in M, \quad w \in M \implies w43 \in M, \dots, \quad w \in M \implies w93 \in M.$$

Proč jsme neumožnili přilepení „13“ je jasné, ale co vynechaná 33? Pokud by se přilepila k řetězci končícím jedničkou, máme problém. Takže takto je to správně. Až na to, že nevytvoříme legitimní řetězec 233. Opět jde o velmi zapeklitý problém. Rozšířený formát umožňuje testovat na poslední znak řetězce takto:

$$w0 \in M \implies w03 \in M, \quad w2 \in M \implies w23 \in M, \quad w3 \in M \implies w33 \in M, \dots, \quad w9 \in M \implies w93 \in M.$$

Je to skvělé, ale není to součástí strukturální indukce coby matematické teorie, takže to používat nebudeme.

△

Musíme se tedy smířit s tím, že některé vzorce strukturální indukce nezvládne. Ale v jiných situacích je výborná. Pomocí pravidel se dá vybudovat například vstupní filtr, který přijme jen správně utvořené výrazy určitého typu. Často nám je zároveň předpřipraví pro další použití tím, že ukáže vnitřní strukturu vstupních dat, například vytvořením odvozovacího stromu. Intuitivně to někdy děláme i my, například když se při derivování komplikovanějšího výrazu rozhodujeme, jaká pravidla pro derivování použít a jakém pořadí. Programy, které umějí derivovat, pracují s odvozovacími stromy. Což nás přivádí k poslednímu příkladu.

Příklad 7c.m: Množinu M korektních algebraických výrazů skládajících se z čísel a malých písmen anglické abecedy lze definovat například takto:

$$(0a) a \in M, b \in M, \dots, z \in M.$$

$$(0b) \alpha \in \mathbb{R} \implies \alpha \in M.$$

$$(1) \text{ Jestliže } \alpha, \beta \in M, \text{ pak } (\alpha) + (\beta) \in M, (\alpha) - (\beta) \in M, (\alpha) \cdot (\beta) \in M, \frac{\alpha}{\beta} \in M, (\alpha)^{(\beta)} \in M, \sqrt{\alpha} \in M.$$

Podle této definice je třeba $(1) + \left(\frac{(a)+(\beta)}{5}\right)$ správně utvořený zápis, ale $\left(\left(1 + \frac{a}{3}\right)^{-5}\right)$ či $3x + -7 + \cdot\sqrt{3}$ nejsou z M .

Čtenáře asi napadlo, že naše pravidla vyžadují zbytečně mnoho závorek, například výraz $2 \cdot a + z$ je správný, ale podle naší definice vytvořit nejde, ta umí jen $((2) \cdot (a)) + (z)$. V našich definicích ale závorky mít musíme, protože kdybychom je třeba v součtu vynechali, tak by někdo takové pravidlo mohl aplikovat na vstupy x a $-y$ a dostal by $x + -y$, což není správný výraz. Optimalizace zápisu by vyžadovala výrazně komplikovanější mechanismus.

△

Takovéto „gramatiky“ se používají například v teorii jazyků (matematických, programovacích). Tento přístup má zajímavé předchůdce. Již cca 500 př.n.l. se hindský učenec jménem Pānini rozhodl sepsat gramatiku sanskritu. Použil na to strukturální indukci a vyšla mu z toho báseň o 3959 verších. Byl to první formální popis přirozeného jazyka v historii.

Cvičení

Cvičení 7c.1 (poučné, zkouškové): Definujte množinu všech neprázdných binárních slov, která:

- neobsahují více nul jdoucích po sobě;
- končí nulou;
- nekončí nulou;
- mají sudý počet znaků;
- mají lichý počet znaků;
- obsahují někde v sobě kombinaci 101.

Cvičení 7c.2 (poučné, zkouškové): Definujte množinu všech slov nad abecedou $C = \{1, 2, 3, 4\}$, která:

- a) neobsahují více trojek jdoucích po sobě;
- b) začínají dvojkou;
- c) nekončí jedničkou.
- d) mají sudý počet znaků;
- e) mají lichý počet znaků.

Pokud to zadání dovoluje, udělejte verzi s prázdným řetězcem λ a verzi bez ní.

Cvičení 7c.3 (poučné, zkouškové): Napište nějakou rekurzivní definici množiny M všech přirozených čísel coby řetězců cifer, které jsou palindromy, tj. čtou se stejně zleva doprava a zprava doleva.

Využijte značení $C = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Pro zjednodušení zde připouštíme čísla, která mají vlevo „zbytečné“ nuly, třeba 01310.

Cvičení 7c.4 (poučné): Napište nějakou rekurzivní definici množiny všech polynomů s reálnými koeficienty.

Nápověda: Indukce může zvyšovat stupeň.

Cvičení 7c.5 (poučné): Napište nějakou rekurzivní definici správných množinových výrazů složených z velkých písmen, \cap , \cup , $-$, $\overline{\quad}$ a závorek.

Cvičení 7c.6 (poučné, dobré): Napište rekurzivní definice těchto množin:

- a) $M = \{(a, b) \in \mathbb{N} \times \mathbb{N}; a + b \text{ liché}\}$;
- b) $M = \{(a, b) \in \mathbb{N} \times \mathbb{N}; a \mid b\}$;
- c) $M = \{(a, b) \in \mathbb{N} \times \mathbb{N}; a \text{ nebo } b \text{ liché}\}$.

Dokažte, že vaše definice jsou správné.

Cvičení 7c.7 (poučné, dobré): Uvažujte množinu M neprázdných řetězců nad $\{a, b, c\}$ zadanou pravidly

- (0) $aa \in M$;
- (1a) $r \in M \implies raa \in M$,
- (1A) $r \in M \implies ara \in M$,
- (1b) $r \in M \implies rb \in M$,
- (1c) $r \in M \implies rc \in M$,
- (1B) $r \in M \implies br \in M$,
- (1C) $r \in M \implies cr \in M$.

Dokažte, že každý řetězec z M obsahuje sudý počet znaků a .

Návod: Uvažujte funkci $f(r)$ na M udávající počet znaků a v řetězci r .

Cvičení 7c.8 (poučné, zkouškové): Uvažujte množinu čísel M definovanou induktivně takto:

- (0) $23 \in M$;
- (1) $m \in M \implies 13 \cdot m \in M$.

Dokažte, že $M = \{n \in \mathbb{N}; \exists k \in \mathbb{N}_0: n = 23 \cdot 13^k\} = \{23 \cdot 13^k; k \in \mathbb{N}_0\}$.

Cvičení 7c.9 (poučné): Použijte strukturální indukci k důkazu, že čísla zadaná

- (0) $a(0, 0) = 0$;
 - (1a) $a(m + 1, 0) = a(m, 0) + 1$ pro $m \in \mathbb{N}_0$,
 - (1b) $a(m, n + 1) = a(m, n) + 1$ pro $m, n \in \mathbb{N}_0$
- splňují $a(m, n) = m + n$ pro $m, n \in \mathbb{N}_0$.

Cvičení 7c.10 (poučné): Použijte strukturální indukci k důkazu, že čísla zadaná

- (0) $a(1, 1) = 5$;
 - (1a) $a(m + 1, 1) = a(m, 1) + 2$ pro $m \in \mathbb{N}$,
 - (1b) $a(m, n + 1) = a(m, n) + 2$ pro $m, n \in \mathbb{N}$
- splňují $a(m, n) = 2(m + n) + 1$ pro $m, n \in \mathbb{N}$.

Řešení:

- 7c.1:** a) (0a) $0 \in M$, (0b) $1 \in M$, (0c) $10 \in M$;
 (1a) $w \in M \implies w1 \in M$, (1b) $w \in M \implies w10 \in M$.

Poznámka: Bez (0c) nelze získat 10 nebo třeba 101.

Alternativa:

- (0a) $0 \in M$ (0b) $1 \in M$, (0c) $01 \in M$;
 (1a) $w \in M \implies 1w \in M$, (1b) $w \in M \implies 01w \in M$.

b) (0) $0 \in M$;

(1a) $w \in M \implies 0w \in M$, (1b) $w \in M \implies 1w \in M$.

Poznámka: Nutno přidávat nalevo, zprava nejde zaručit správné ukončení.

c) (0) $1 \in M$;

(1a) $w \in M \implies 0w \in M$, (1b) $w \in M \implies 1w \in M$.

Poznámka: Nutno přidávat nalevo, zprava nejde zaručit správné ukončení.

d) (0a) $00 \in M$, (0b) $01 \in M$, (0c) $10 \in M$, (0d) $11 \in M$;

(1a) $w \in M \implies w00 \in M$, (1b) $w \in M \implies w01 \in M$, (1c) $w \in M \implies w10 \in M$,

(1d) $w \in M \implies w11 \in M$.

e) (0a) $0 \in M$, (0b) $1 \in M$;

(1a) $w \in M \implies w00 \in M$, (1b) $w \in M \implies w01 \in M$, (1c) $w \in M \implies w10 \in M$,

(1d) $w \in M \implies w11 \in M$.

f) (0) $101 \in M$;

(1a) $w \in M \implies 0w \in M$, (1b) $w \in M \implies 1w \in M$, (1c) $w \in M \implies w0 \in M$,

(1d) $w \in M \implies w1 \in M$.

7c.2: a) (0a) $c \in C \implies c \in M$, (0b) $c \in C - \{3\} \implies c3 \in M$;

(1a) $w \in M, c \in C - \{3\} \implies wc \in M$, (1b) $w \in M, c \in C - \{3\} \implies wc3 \in M$.

Poznámka: Bez (0b) nelze získat 13.

Alternativa: a) (0a) $\lambda \in M$, (0b) $3 \in M$;

(1a) $w \in M, c \in C - \{3\} \implies wc \in M$, (1b) $w \in M, c \in C - \{3\} \implies wc3 \in M$.

Poznámka: V obou případech možná i verze s přidáváním zleva.

b) (0) $2 \in M$; (1) $w \in M, c \in C \implies wc \in M$.

Poznámka: Nutno přidávat napravo, zleva nejde zaručit správné ukončení.

Zadání nepřipouští λ .

c) (0) $c \in C - \{1\} \implies c \in M$; (1) $w \in M, c \in C \implies cw \in M$.

Poznámka: Nutno přidávat nalevo, zprava nejde zaručit správné ukončení.

Alternativa:

(0a) $\lambda \in M$, (0b) $c \in C - \{1\} \implies c \in M$; (1) $w \in M, c \in C \implies cw \in M$.

d) (0) $c, d \in C \implies cd \in M$; (1) $w \in M, c, d \in C \implies wcd \in M$.

Poznámka: Verze s přidáváním zleva také možná, také verze s přidáváním cwd .

Alternativa:

(0) $\lambda \in M$; (1) $w \in M, c, d \in C \implies wcd \in M$.

Poznámka: Verze s přidáváním zleva také možná, také verze s přidáváním cwd .

e) (0) $c \in C \implies c \in M$; (1) $w \in M, c, d \in C \implies wcd \in M$.

Poznámka: Verze s přidáváním zleva také možná, také verze s přidáváním cwd .

Verze s λ zde nedává smysl.

7c.3: (0a) $c \in C \implies c \in M$, (0b) $c \in C \implies cc \in M$; (1) $w \in M, c \in C \implies cwc \in M$.

7c.4: (0) $a \in \mathbb{R} \implies a \in P$; (1) $p \in P, a \in \mathbb{R} \implies x \cdot p + a \in P$.

Alternativa (méně elegantní): (1) $p \in P, a \in \mathbb{R}, n \in \mathbb{N} \implies p + ax^n \in P$.

Poznámka: Proč by nefungovala definice (1) $p \in P, a \in \mathbb{R} \implies (x - a) \cdot p \in P$? Což takhle $x^2 + 1$?

7c.5: (0) $A, B, \dots, Z \in \mathcal{M}$;

(1a) $v \in \mathcal{M} \implies \bar{v} \in \mathcal{M}$, (1b) $v_1, v_2 \in \mathcal{M} \implies (v_1 \cup v_2) \in \mathcal{M}$,

(1c) $v_1, v_2 \in \mathcal{M} \implies (v_1 \cap v_2) \in \mathcal{M}$, (1d) $v_1, v_2 \in \mathcal{M} \implies (v_1 - v_2) \in \mathcal{M}$.

7c.6: a) (0) $(2, 1) \in S$, $(2, 1) \in S$;

(1a) $(a, b) \in S \implies (a + 2, b) \in S$, (1b) $(a, b) \in S \implies (a, b + 2) \in S$.

$S \subseteq M$ strukturální indukci: (0) $1 + 2 = 3$ liché, proto $(1, 2), (2, 1) \in M$.

(1) Předpoklad: $(a, b) \in S$ splňuje $(a, b) \in M$. Pak $a + b$ je liché a tudíž je i $a + b + 2$ liché, proto prvky ze závěru

(1a) a (1b) splňují $(a + 2, b) \in M$ a $(a, b + 2) \in M$.

$M \subseteq S$ nejlépe slabou indukci na $a + b$. Vlastnost $V(n)$: Každá dvojice $(a, b) \in \mathbb{N}^2$ s vlastností $a + b = 2n + 1$ leží v S . Protože $a, b \geq 1$, je nejmenší možný lichý součet 3, proto bereme $n \geq 1$.

(0) $n = 1$: Jestliže $a + b = 3$, pak z $a, b \in \mathbb{N}$ plyne, že $(a, b) = (1, 2)$ nebo $(a, b) = (2, 1)$, každopádně dle (0) v definici $(a, b) \in S$.

(1) Předpokládáme platnost pro jisté $n \in \mathbb{N}$. Nechť $(a, b) \in \mathbb{N}^2$ splňuje $a + b = 2(n + 1) + 1 = 2n + 3$. Pak $a + b \geq 5$ a proto je alespoň jedno z čísel a, b větší než 2. Možnost $a \geq 3$: Pak $(a - 2, b) \in \mathbb{N}^2$ a $(a - 2) + b = 2n + 1$, proto dle indukčního předpokladu $(a - 2, b) \in S$. Pak ale dle (1a) také $(a, b) = ((a - 2) + 2, b) \in S$. Možnost $b \geq 3$ obdobně.

b) (0) $(1, 1) \in S$;

(1a) $[(a, b) \in S \wedge c \in \mathbb{N}] \implies (ac, bc) \in S$, (1b) $[(a, b) \in S \wedge c \in \mathbb{N}] \implies (a, bc) \in S$.

$S \subseteq M$ lehce strukturální indukci. $M \subseteq S$ nejlépe ve dvou krocích. V prvním kroku indukci na a dokázat, že $(a, a) \in S$. V druhém kroku silnou indukci na $\frac{b}{a}$ dokázat $M \subseteq S$.

c) (0) $(1, 1) \in S, (1, 2) \in S, (2, 1) \in S$;

(1a) $(a, b) \in S \implies (a + 2, b) \in S, \quad (1b) (a, b) \in S \implies (a, b + 2) \in S$.

$S \subseteq M$ lehce strukturální indukci. $M \subseteq S$ nejlépe silnou indukci na $a + b$, protože $a + b - 2$ znamená, že $a - 2$ či $b - 2$ má stejnou paritu jako a či b , tedy z lichého bude liché.

7c.7: Uvažujme $f(r)$ na M udávající počet znaků a v řetězci r . Dokážeme, že f má v M sudé hodnoty.

Strukturální indukce. (0) V pravidle (0_D) vznikají prvky aa , pro ně $f(aa) = 2$.

(1) Nechť r je prvek z M , indukční předpoklad je, že $f(r)$ je sudé.

Pak pro prvek vzniklý z (1a) platí $f(raa) = f(r) + 2$, což je také sudé. Pro prvek vzniklý z (1A) platí $f(ara) = f(r) + 2$, což je také sudé. Pro prvek vzniklý z (1b) platí $f(rb) = f(r)$, což je také sudé. Podobně pro ostatní pravidla.

7c.8: Dvě inkluze

1) $W(k): 23 \cdot 13^k \in M$ indukci (slabým principem):

(0) $k = 0: 23 \cdot 13^0 = 23 \in M$ dle (0_D) .

(1) $k \in \mathbb{N}_0$, nechť $W(k)$ platí, tedy $23 \cdot 13^k \in M$. Pak podle (1_D) je v M také $13 \cdot 23 \cdot 13^k = 23 \cdot 13^{k+1}$, tedy $W(k+1)$ platí.

Proto W platí pro všechna $k \in \mathbb{N}_0$ a $\{23 \cdot 13^k; k \in \mathbb{N}_0\} \subseteq M$.

2) $V(m)$ vlastnost, že pro $m \in M$ existuje $k \in \mathbb{N}_0: m = 23 \cdot 13^k$. Důkaz strukturální indukci, že $V(m)$ platí pro všechna $m \in M$.

(0) Základní pravidlo obsahuje jen 23, a $23 = 23 \cdot 13^0$. V platí pro prvky ze základního kroku.

(1) Vezměme prvek $m \in M$ z předpokladu indukčního pravidla. Předpoklad: V pro něj platí, tj. existuje $k \in \mathbb{N}_0$ splňující $m = 23 \cdot 13^k$. Závěr pravidla do M dává prvek $13m$. Pro něj máme $13m = 13 \cdot 23 \cdot 13^k = 23 \cdot 13^{k+1}$, tedy i pro něj platí V .

Podle (0), (1) a strukturální indukce V platí pro všechna $m \in M$, tedy $M \subseteq \{23 \cdot 13^k; k \in \mathbb{N}_0\}$.

7c.9: Definujme množinu $M = \mathbb{N}_0^2$ strukturální indukci takto:

(0) $(0, 0) \in M; \quad (1a) (m, 0) \in M \implies (m + 1, 0) \in M, \quad (1b) (m, n) \in M \implies (m, n + 1) \in M$.

Vlastnost $V(m, n)$ na množině M : pro $(m, n) \in M$ platí $a(m, n) = m + n$. Platnost dokážeme strukturální indukci dle definice M :

(0) Pro prvek $a(0, 0) = 0$ to platí.

(1) Pravidlo (1a): Předpokládejme, že $V(m, n)$ platí pro prvek $(m, 0) \in M$, tedy $a(m, 0) = m + 0 = m$. Pak dle (1a) platí $a(m + 1, 0) = a(m, 0) + 1 = (m + 1) + 0$, tedy $V(m, n)$ platí také pro prvek $(m + 1, 0)$.

Pravidlo (1b): Předpokládejme, že $V(m, n)$ platí pro prvek $(m, n) \in M$, tedy $a(m, n) = m + n$. Pak dle (1b) platí $a(m, n + 1) = a(m, n) + 1 = m + (n + 1)$, tedy $V(m, n)$ platí také pro prvek $(m, n + 1)$.

7c.10: Definujme množinu $M = \mathbb{N}^2$ strukturální indukci takto:

(0) $(1, 1) \in M; \quad (1a) (m, 1) \in M \implies (m + 1, 1) \in M, \quad (1b) (m, n) \in M \implies (m, n + 1) \in M$

Vlastnost $V(m, n)$ na množině M : pro $(m, n) \in M$ platí $a(m, n) = 2(m + n) + 1$. Platnost dokážeme strukturální indukci dle definice M :

(0) Pro prvek $a(1, 1) = 5$ to platí, $5 = 2 \cdot (1 + 1) + 1$.

(1) Pravidlo (1a): Předpokládejme, že $V(m, n)$ platí pro prvek $(m, 1) \in M$, tedy $a(m, 1) = 2(m + 1) + 1 = 2m + 3$. Pak dle (1a) platí $a(m + 1, 1) = a(m, 1) + 2 = 2m + 5 = 2((m + 1) + 1) + 1$, tedy $V(m, n)$ platí také pro prvek $(m + 1, 1)$.

Pravidlo (1b): Předpokládejme, že $V(m, n)$ platí pro prvek $(m, n) \in M$, tedy $a(m, n) = 2(m + n) + 2 = 2m + 2n + 2$. Pak dle (1b) platí $a(m, n + 1) = a(m, n) + 2 = 2m + 2n + 4 = 2(m + (n + 1)) + 2$, tedy $V(m, n)$ platí také pro prvek $(m, n + 1)$.

7d. Indukce a teorie

V této kapitole si položíme klíčovou otázku: Jak vlastně víme, že principy indukce fungují? Začneme tím, co už naznačily naše příklady. U silného i modifikovaného principu jsme příslušný inspirační příklad řešili také slabou indukci pomocí pomocné vlastnosti. Funguje to obecně. Ukážeme, že silný ani modifikovaný princip vlastně nepřinášejí nic navíc, tedy kromě pohodlí. Protože „modifikovaný princip“ není běžně zaváděn, formulujeme to pro princip silný.

Věta 7d.1.

Slabý a silný princip matematické indukce jsou ekvivalentní.

Tím říkáme následující: Pokud platí jeden, pak platí i druhý a naopak. Z praktického pohledu to znamená, že vlastnosti, které jdou dokázat slabým principem, jdou dokázat i tím silným, a naopak.

Důkaz (poučný, drsný): $1 \implies$: Předpokládejme, že platí slabý princip indukce. Ukážeme, že platí i silný.

Uvažujme tedy $n_0 \in \mathbb{Z}$ a nějakou vlastnost $V(n)$ definovanou pro $n \geq n_0$, která splňuje:

(S0) $V(n_0)$ platí.

(S1) Pro všechna $n \geq n_0$: Jestliže platí $V(n_0), V(n_0 + 1)$ až $V(n)$, tak platí i $V(n + 1)$.

Potřebujeme ukázat, že pak $V(n)$ platí pro všechna $n \geq n_0$ neboli že silný princip funguje.

Použijeme přístup z příkladu 7b.b. Uvažujme vlastnost W definovanou pro $n \geq n_0$ takto: $W(n)$ platí právě tehdy, když platí $V(k)$ pro $n_0 \leq k \leq n$. Ukážeme, že tato vlastnost W splňuje předpoklady slabého principu:

(s0) $n = n_0$: Dle (S0) předpokládáme platnost $V(n_0)$, což je přesně platnost $W(n_0)$.

(s1) Dáno $n \geq n_0$. Předpoklad: $W(n)$ platí. Pak podle definice W platí $V(n_0)$ až $V(n)$, proto podle předpokladu (S1) platí i $V(n + 1)$. Takže platí $V(n_0)$ až $V(n + 1)$ neboli platí $W(n + 1)$. Implikace $W(n) \implies W(n + 1)$ potvrzena.

Protože W splňuje předpoklady slabého principu, o kterém předpokládáme, že platí, musí platit i jeho závěr, tedy $W(n)$ platí pro všechna $n \geq n_0$. Podle definice této vlastnosti tedy platí $V(n)$ pro všechna $n \geq n_0$.

Ukázali jsme, že pokud V splňuje (S0) a (S1), tak V platí všude, tedy platí silný princip indukce.

$2 \implies$: Předpokládejme, že platí silný princip indukce. Ukážeme, že platí i slabý.

Uvažujme tedy $n_0 \in \mathbb{Z}$ a nějakou vlastnost $V(n)$ definovanou pro $n \geq n_0$, která splňuje:

(s0) $V(n_0)$ platí.

(s1) Pro všechna $n \geq n_0$: Jestliže platí $V(n)$, tak platí i $V(n + 1)$.

Potřebujeme ukázat, že pak $V(n)$ platí pro všechna $n \geq n_0$ neboli že slabý princip funguje.

Potvrdíme, že tato vlastnost V splňuje i podmínky silného principu.

(S0) $n = n_0$: Platnost $V(n_0)$ vyplývá z (s0).

(S1) Dáno $n \geq n_0$. Předpoklad: Platí $V(n_0)$ až $V(n)$. Pak mimo jiné platí $V(n)$ a podle (s1) musí platit $V(n + 1)$. Implikace $[V(n_0) \wedge \dots \wedge V(n)] \implies V(n + 1)$ potvrzena.

Protože V splňuje předpoklady silného principu, o kterém předpokládáme, že platí, musí platit i jeho závěr, tedy $V(n)$ platí pro všechna $n \geq n_0$.

Ukázali jsme, že pokud V splňuje (s0) a (s1), tak V platí všude, tedy platí slabý princip indukce. □

Ekvivalence modifikovaného principu se dokazuje obdobně. V jednom směru je to snadné, protože když v modifikovaném principu použijeme hodnotu $m = 1$, tak dostáváme přímo slabý princip indukce. Důkaz opačného směru opět využívá pomocnou vlastnost W , podobně jako v příkladě 7b.h. Přesně, řekli bychom, že $W(n)$ platí právě tehdy, pokud platí $V(n), V(n - 1)$ až $V(n - m + 1)$. Details necháme čtenáři.

Další na řadě je strukturální indukce.

Věta 7d.2.

Princip strukturální indukce vyplývá z principu matematické indukce.

Důkaz (drsný): Předpokládejme, že platí silný princip indukce. Ukážeme, že pak platí princip strukturální indukce.

Uvažujme tedy nějakou množinu M danou základními pravidly (0i) a indukčními pravidly (1j). Uvažujme také vlastnost V definovanou na M a splňující předpoklady strukturální indukce:

(s0) V platí pro všechny prvky základních kroků.

(s1j) Jestliže je V splněna pro všechny prvky z předpokladu j -tého pravidla, pak platí i pro prvek z jeho závěru.

Ukážeme pomocí silného principu indukce, že V pak musí platit pro všechny prvky z M . Definujme proto novou vlastnost $W(n)$ na \mathbb{N} takto: $W(n)$ platí, jestliže je V splněno pro všechny prvky M s výškou n .

Tvrdíme, že tato vlastnost W splňuje předpoklady silného principu matematické indukce.

(S0): Nechť $n = 1$. $W(1)$ platí, pokud je V splněno pro všechny prvky M výšky jedna, tedy prvky ze základních pravidel. To ale platí dle (s0).

(S1): Předpokládejme, že platí $W(1)$ až $W(n)$. To znamená, že V platí pro všechny prvky množiny M , jejichž výška je nejvýše n .

Platí $W(n + 1)$? Máme ukázat, že V platí pro všechny prvky množiny M výšky $n + 1$. Vezměme tedy jeden takový prvek m . Protože je to prvek z M a má výšku $n + 1 > 1$, tak se v M ocitnul na základě nějakého indukčního pravidla. Vezměme tedy jeho derivační strom, který dává výšku $n + 1$, a vidíme, že m vzniklo použitím nějakého indukčního pravidla (1j). Toto pravidlo má ve svém předpokladu nějaké prvky $m_i \in M$, které se v našem derivačním stromě pro m objeví o úroveň výš. Mají proto derivační strom, jehož výška je

určitě menší než výška pro m , tedy všechny m_i mají výšku nejvýše n . Podle indukčního předpokladu pro ně V platí, a proto podle předpokladu (s1j) strukturální indukce musí V platit i pro prvek m , přesně jak jsme potřebovali.

$W(n+1)$ tedy platí. Ukázali jsme, že W splňuje (S0) a (S1), proto podle silného principu matematické indukce $W(n)$ platí pro všechna n , tedy V platí pro všechny prvky M . □

Naopak je to trochu složitější. Pokud platí princip strukturální indukce a akceptujeme Peanovu definici přirozených čísel, tak zjevně platí také slabý princip indukce a tedy všechny klasické indukční principy.

Tedy víme, že buď naše principy všechny platí, nebo naopak všechny neplatí. Jak to tedy s nimi je? Pravda je taková, že je to jeden z axiomů matematiky, tedy platnost indukce můžeme přijmout, nebo také ne. Standardně se přijímá, ovšem mezi obvyklými axiomy princip indukce nenajdeme, protože už tam je v převleku, viz Princip 6b.16.

Věta 7d.3.

Princip matematické indukce je ekvivalentní s principem dobrého uspořádání.

Důkaz (drsný, poučný): Ukážeme ekvivalenci principu dobrého uspořádání se silným principem indukce.

1) \implies : Předpokládejme, že platí silný princip matematické indukce. Chceme ukázat, že (\mathbb{N}, \leq) je dobře uspořádaná množina.

Nechť je tedy M nějaká neprázdná podmnožina \mathbb{N} . Uvažujme pro $n \in \mathbb{N}$ vlastnost $n \notin M$.

Protože $M \neq \emptyset$, nemůže tato vlastnost platit pro všechna $n \in \mathbb{N}$, podle silného principu tedy nemohou platit zároveň obě následující tvrzení:

(0) $1 \notin M$;

(1) Pro každé $n \in \mathbb{N}$: Jestliže $k \notin M$ pro $k \in \{1, \dots, n\}$, pak $(n+1) \notin M$.

Jestliže není pravda (0), tak $1 \in M$. Jelikož $M \subseteq \mathbb{N}$, tak $1 \leq x$ pro všechna $x \in M$, tedy 1 je nejmenší prvek M .

Druhá možnost je, že neplatí (1). To znamená, že existuje $n \in \mathbb{N}$ takové, že platí předpoklad implikace, tedy $1 \notin M$, $2 \notin M$ až $n \notin M$, ale neplatí závěr, tedy platí $n+1 \in M$.

Protože M neobsahuje čísla $1, 2, \dots, n$, tak pro všechna $x \in M$ máme $n+1 \leq x$. Toto a závěr předchozího odstavce ukazují, že $n+1$ je nejmenší prvek M .

Rozborem možností jsme ukázali, že M má za všech okolností nejmenší prvek.

Všechny neprázdné podmnožiny \mathbb{N} mají nejmenší prvek vzhledem k \leq , tedy (\mathbb{N}, \leq) je dobře uspořádaná.

2) \impliedby : Předpokládejme, že platí princip dobrého uspořádání. Z toho vyplývá, že pro každé $n_0 \in \mathbb{Z}$ je

$$M = \{n \in \mathbb{Z}; n \geq n_0\}$$

dobře uspořádaná množina vzhledem k relaci \leq , viz příklad 6b.n.

Ověříme, že platí silný princip inkluze.

Zvolme $n_0 \in \mathbb{Z}$ a uvažujme nějakou vlastnost V na odpovídající množině M . Předpokládejme, že splňuje následující:

(S0) $V(n_0)$ platí.

(S1) Pro každé $n \in M$: Jestliže platí $V(n_0), \dots, V(n)$, pak platí i $V(n+1)$.

Potřebujeme ukázat, že pak V platí na M . Uvažujme podmnožinu

$$N = \{n \in M; V(n) \text{ neplatí}\}.$$

Ukážeme sporem, že je prázdná.

Pokud by N prázdná nebyla, tak by podle principu dobrého uspořádání (M, \leq) musela mít nejmenší prvek $m \in N$. Pokud $m = n_0$, tak by $V(n_0)$ neplatilo, což je ve sporu s (S0).

Pokud $m > n_0$, tak čísla n_0 až $m-1$ neleží v N , tedy platí $V(n_0)$ až $V(m-1)$. Díky $m > n_0$ neboli $m-1 \geq n_0$ je možné aplikovat (S1), proto $V(m)$ neplatí, což je ve sporu s $m \in N$.

Ukázali jsme, že $N = \emptyset$, a proto V platí na M .

Dokázali jsme, že z podmínek (S0) a (S1) plyne platnost V všude neboli platí silný princip inkluze. □

Dobrá otázka: Proč jsme v části 1) nepoužili obvyklý trik a nedokazovali indukci $V(n)$: každá n -prvková podmnožina \mathbb{N} má minimum? Protože definice dobrého uspořádání zahrnuje i minima nekonečných podmnožin, takže by to nestačilo. S tím se ale dá vyrovnat, možných přístupů je víc, takže lze porůznu najít také jiné důkazy této věty. Ten náš je zajímavý tím, že využívá princip indukce v situaci, kdy dokazovaná vlastnost neplatí.

Přirozeným zobecněním je podívat se na obecné dobře uspořádané množiny.

Věta 7d.4. (o dobře uspořádané indukci)

Nechť (A, \preceq) je dobře uspořádaná množina, \prec její odvozené ostré uspořádání. Nechť $V(a)$ je vlastnost prvků $a \in A$.

Předpokládejme, že je splněna následující podmínka zvaná **indukční krok**:

(I) Pro všechna $a \in A$: Jestliže $V(x)$ platí pro všechna $x \in A$ splňující $x \prec a$, pak platí také $V(a)$.

Pak platí $V(a)$ pro všechna $a \in A$.

Důkaz (poučný): Použijeme nepřímý důkaz neboli dokážeme obměnu: Pokud není pravda, že vlastnost V platí na množině A , tak pro ni také nemůže platit (I).

Jestliže není V vždy splněno, pak je množina $M = \{y \in A; V(y) \text{ neplatí}\}$ neprázdná a díky dobrému uspořádání má svůj nejmenší prvek, nazvěme jej a . Ukážeme, že pro něj neplatí (I).

Uvažujme množinu $X = \{x \in A; x \prec a\}$ předchůdců a . Chceme ukázat, že neplatí následující:

(I) Jestliže $V(x)$ platí pro všechna $x \in X$, pak platí také $V(a)$.

Důkaz neplatnosti (I) rozdělíme na dva případy. Pokud je X prázdná, tak je předpoklad implikace automaticky splněn, ale neplatí závěr $V(a)$ a implikace (I) neplatí.

Druhá možnost je, že X prázdná není. Všechny prvky $x \in X$ splňují $x \prec a$, proto podle faktu 6a.3 (ii) nemohou splňovat $a \preceq x$. Nemohou tak být v M , protože a je nejmenší prvek M a tedy pro $y \in M$ platí $a \preceq y$. Jelikož prvky z X nejsou v M , znamená to, že pro $x \in X$ platí $V(x)$ a je splněn předpoklad implikace (I). Ovšem a coby nejmenší prvek M v této množině leží, tedy $V(a)$ neplatí, a proto neplatí ani implikace (I).

Takže ve všech případech (I) neplatí a důkaz je hotov. □

Tato indukce je zvláštní v tom, že má jen jeden krok. Ve skutečnosti je tam i základní krok (0), ale zamaskovaně. Je to vidět v důkazu výše.

Představme si, že chceme na množině A dokázat nějakou vlastnost pomocí podmínky (I). Potřebujeme dokázat platnost příslušné implikace pro všechny prvky a , což se nutně rozpadne na dva případy.

Pokud a nemá předchůdce, tak je předpoklad implikace (I) automaticky splněn. Abychom ukázali její platnost, musíme ukázat platnost $V(a)$ přímo, bez pomoci od předchozích případů. To přesně odpovídá tradičnímu kroku (0), tedy přímo dokazujeme platnost V pro prvky a bez předchůdců.

Pokud a má předchůdce, tak se pomocí informace, že splňují V , musíme dostat k tomu, že také a splňuje V . To odpovídá klasickému kroku (1).

V praxi se tedy (I) chová jako (0) nebo (1) podle typu a .

Pro běžného čtenáře je toto maskování spíš na obtíž, ale matematictí nadšenci ocení eleganci, se kterou jsme celý proces indukce schovali do jednoho stručného vyjádření.

Existuje ještě obecnější verze tohoto tvrzení. Lze dokázat, že princip matematické indukce platí na uspořádané množině (A, \preceq) právě tehdy, když je tato množina fundovaná neboli nemůže obsahovat nekonečnou klesající posloupnost (viz 6c). Což nás přivádí k ještě jednomu indukčnímu principu, který se někdy používá, ukážeme verzi pro \mathbb{N} . Česky se mu říká „sestupná indukce“.

7d.5. Princip sestupné indukce (Infinite descent proof).

Nechť $V(n)$ je vlastnost přirozených čísel.

Předpokládejme, že splňuje následující:

(1) Pro každé $n \in \mathbb{N}$ je pravdivá implikace:

Jestliže neplatí $V(n)$, pak existuje $k \in \mathbb{N}$ takové, že $k < n$ a $V(k)$ neplatí.

Potom $V(n)$ platí pro všechna $n \in \mathbb{N}$.

Argument, proč toto funguje, je následující: Kdyby náhodou $V(n)$ neplatilo pro nějaké n , tak by to podle (1) muselo platit i pro menší číslo, takže podle (1) pro ještě menší číslo a tak dále, čímž by vznikla nekonečná klesající posloupnost v \mathbb{N} . To ovšem není možné, protože \mathbb{N} je dobře uspořádaná a tedy fundovaná, viz poznámka 6c.3.

Tento argument je platný i obecně, v případě \mathbb{N} se lze k tomuto principu dostat přímo z principu silné indukce. Začneme tím, že jeho podmínky (0) a (1) sloučíme do jedné, jak jsme to viděli výše:

(I) Jestliže platí $V(k)$ pro všechna $k < n$, $k \in \mathbb{N}$, tak platí $V(n)$.

Ta má být platná pro všechna $n \in \mathbb{N}$. Přechodem k obměně dostáváme ekvivalentní verzi

(I) Jestliže neplatí $V(n)$, pak nemůže $V(k)$ platit pro všechna $k < n$, $k \in \mathbb{N}$.

Vidíme, že princip sestupné indukce je vlastně jen přepisem silné indukce a je tedy zase ekvivalentní klasickým indukčním principům.

Mnohdy se používá intuitivně. Postupuje se sporem: Předpokládá se, že pro číslo a_k něco neplatí, pomocí čehož se přejde k číslu a_{k+1} , které je menší než a_k . Protože $a_k \in \mathbb{N}$ a tvoří klesající posloupnost, tak se zdá zjevné, že proces se někde zastaví a nastane spor. My už ovšem víme, že ta zjevnost je vlastně axiom.

Poznamenali jsme, že přechodem k negaci lze vlastnosti také indukcí vyvracet. Zrovna u tohoto principu je to populární a někdy tak také bývá uváděn:

- Předpokládejme, že vlastnost $V(n)$ přirozených čísel splňuje pro každé $n \in \mathbb{N}$ následující:

Jestliže platí $V(n)$, pak existuje $k \in \mathbb{N}$ takové, že $k < n$ a $V(k)$ platí.

Potom $V(n)$ neplatí pro žádné $n \in \mathbb{N}$.

Příklad 7d.a: Tento princip použil už Euklid k důkazu, že $\sqrt{2}$ není racionální číslo. Definujme tuto vlastnost:

- $V(n)$: existuje přirozené číslo p splňující $\sqrt{2} = \frac{p}{n}$.

To, že $\sqrt{2} \notin \mathbb{Q}$, je ekvivalentní právě tomu, že $V(n)$ není splněno pro žádné $n \in \mathbb{N}$.

Dokážeme to sestupnou indukcí. Pokud by platilo $V(n)$, tak $\sqrt{2} = \frac{p}{n}$. Pak $2 = \frac{p^2}{n^2}$ neboli $p^2 = 2n^2$. To znamená, že 2 dělí p^2 , a protože je 2 prvočíslo, musí dělit rovnou p . Máme tedy $p = 2a$ pro nějaké $a \in \mathbb{N}$. Pak $4a^2 = 2n^2$ a stejným argumentem ukážeme, že také 2 dělí n , tudíž $n = 2k$ pro nějaké $k \in \mathbb{N}$. Pak jde ve zlomku zkrátit a máme $\sqrt{2} = \frac{a}{k}$. Našli jsme tedy $k \in \mathbb{N}$ takové, že $k < n$ a $V(k)$ platí.

Podle principu sestupné indukce to již dokazuje, že žádné $V(n)$ nemůže platit.

△

Sestupná i klasická indukce hrají významnou roli v analýze algoritmů.

! Příklad 7d.b:

Když navrhne nějaký algoritmus, tak bychom správně měli dokázat, že vždy dělá to, co má. Přesněji řečeno, chceme, aby se pro libovolné vstupy algoritmus po konečném počtu kroků zastavil a dal správný výstup. Jde vlastně o dva požadavky, které se pro zjednodušení situace typicky zkoumají každý zvlášť.

Odborný název *parciální korektnost* znamená, že pokud daný algoritmus skončí, tak dá správný výstup. Zajímavým nástrojem je **invariant**, což je nějaký ukazatel, který souvisí s žádaným výstupem a u kterého lze dokázat, že se v jednotlivých krocích algoritmu nemění. To je obvykle příležitost pro indukci, viz například důkaz, že Euklidův algoritmus poskytne $\text{gcd}(a, b)$, v kapitole 14.

Indukce se uplatní zejména u rekurentních algoritmů i v případě, že invariant nepoužijeme. Uvažujme následující algoritmus.

```
procedure factorial(n: nezáporné celé číslo)
  if n = 0 then factorial(n) := 1
  else factorial(n) := n · factorial(n - 1);
```

Tvrdíme, že výstup procedury je $n!$. Dokážeme to pro $n \geq 0$ indukcí.

(0) $n = 0$: ano, podle specifikace je $\text{factorial}(0) = 1 = 0!$.

(1) Nechť $n \in \mathbb{N}_0$. IP: výstup $\text{factorial}(n)$ je $n!$. Pak výstup $\text{factorial}(n + 1)$ je roven $(n + 1) \cdot \text{factorial}(n)$, což podle IP je $(n + 1) \cdot n! = (n + 1)!$.

□

To ovšem platí jen tehdy, pokud k nějakému výstupu dojde neboli pokud algoritmus skončí. Zkusme si představit, že onen algoritmus výše poštve na číslo 1.7. Náš algoritmus zjistí, že to není nula, tudíž zavolá sám sebe znovu, tentokrát se vstupem 0.7. To zase není nula, tudíž se zavolá se vstupem -0.3 . A tak dále, program nikdy neskončí.

Čtenář patrně namítne, že jsme špatní programátoři, protože jsme zapomněli doplnit vstupní filtr. To je pravda, jenže jsme měli snadný algoritmus. Pokud je komplikovanější, tak vůbec nemusí být jasné, co je tím vhodným vstupním filtrem.

Snad každý rekurentní algoritmus má množinu základních hodnot, které umí rovnou, vypíše výsledek a skončí. Pokud dostane hodnotu jinou, tak ji všelijak upravuje a sám sebe spouští znovu a znovu, dokud se netrefí do jedné z těch základních hodnot. Podobně fungují algoritmy, které mají smyčku čekající na správný výsledek. Ostatně i ten faktoriál bychom mohli získat také jiným programem (dokonce by to bylo žádoucí, protože rekurze je elegantní, ale z praktického pohledu problematická).

```
procedure factorial(n: nezáporné celé číslo)
  a := 1;
  while n > 0 do
    a := a · n;
    n := n - 1;
  output: a;
```

Člověk by řekl, že vzhledem ke zmenšujícímu se n se musí dříve či později dojit k situaci, kdy $n > 0$ neplatí, a algoritmus skončí.

Zde se vlastně odvoláváme na princip sestupné indukce 7d.5, použila by se vlastnost $V(n)$: algoritmus se po cyklu s indexem n nezastaví.

To je inspirace pro oblíbený typ důkazu, že se algoritmus jistě dříve či později zastaví. Pokud se podaří vygenerovat nějaký ukazatel r_k , tradičně zvaný **variant**, který je z \mathbb{N} či \mathbb{N}_0 a při každém volání rekurze či každém průběhu cyklu se zmenší, tak algoritmus nutně musí skončit. Jinak by se totiž vyrobila nekonečná klesající posloupnost $r_1 > r_2 > r_2 > \dots$ přirozených čísel.

Ovšem ne vždy se to povede a k setkání s problémem ani není třeba něco komplikovaného. Uvažujme následující zobrazení $T: \mathbb{N} \mapsto \mathbb{N}$ dané předpisem

$$T(n) = \begin{cases} \frac{1}{2}n, & n \text{ sudé;} \\ 3n + 1, & n \text{ liché.} \end{cases}$$

Je to jednoduchý předpis, třeba $T(8) = \frac{1}{2}8 = 4$ (8 je sudé) a $T(13) = 3 \cdot 13 + 1 = 40$ (13 je liché).

Zajímavá otázka zní, co se stane, když T začneme aplikovat opakovaně (neboli když uvažujeme mocniny T^m tohoto zobrazení). Když třeba začneme s $n = 13$, tak máme $T(13) = 40$. To je sudé, takže další aplikace T dává $T^2(13) = T(40) = \frac{1}{2}40 = 20$. To je zase sudé, tedy $T^3(13) = T(20) = 10$, pak $T^4(13) = 5$ a tak dále, dostáváme řetězec

$$13 \mapsto 40 \mapsto 20 \mapsto 10 \mapsto 5 \mapsto 16 \mapsto 8 \mapsto 4 \mapsto 2 \mapsto 1,$$

tedy $T^9(13) = 1$.

Lidé si myslí, že ať už začneme jakýmkoliv n , vždycky dřív nebo později dojdeme k 1. Zatím to ale nikdo neuměl ani dokázat, ani vyvrátit, takže se to prostě neví. Což nás přivádí k tomuto algoritmu:

```
procedure T(n: přirozené číslo)
while n > 1 do;
  if n even then n := 1/2 n
  else n := 3n + 1;
output: n;
```

Toto je jednoduchý rekurzivní program, který, pokud jej zavoláme jako $T(13)$, skončí po devíti cyklech. Pokud se zastaví, tak dá výstup 1, což je cílem, je tedy parciálně korektní. Jenže my nevíme, zda se zastaví.

Terminální podmínku má ($n = 1$), ale z toho, co jsme o zobrazení T řekli, vyplývá, že není známo, zda k ní pro všechna vstupní data tento program někdy dojde. To je smutné, současná věda neumí u tohoto algoritmu dokázat, že vždy skončí. Což mimo jiné znamená, že pro něj zatím nikdo neuměl vymyslet variant.

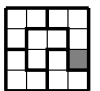
△

7e. Bonus: Další důkazy indukcí

Zde ukážeme některé další zajímavé aplikace indukce.

Příklad 7e.a: Uvažujme čtvercovou šachovnici se stranou o velikosti 2^n polí.

Jinak řečeno, uvažujme čtverec zformovaný z $(2^n)^2$ malých čtverců, kde $n \in \mathbb{N}$. Začerníme jedno z polí. Tvrdíme, že to, co zbyde, lze zcela pokrýt dlaždicemi složenými ze 3 čtverečků ve tvaru L (tzv. trimin, viz obrázek) tak, aby se nepřekrývaly.



Důkaz provedeme to matematickou indukcí.

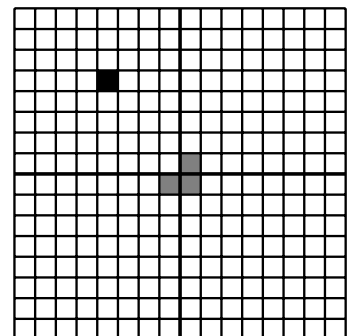
(0) Je-li $n = 1$, pak jde o čtverec o straně $2^1 = 2$. Po začernění jednoho pole ve čtverci 2×2 zbude právě jedno trimino, které samozřejmě triminy vydláždíme.

(1) Vezměme libovolné $n \in \mathbb{N}$ a předpokládejme, že umíme vydláždit „čtverec 2^n minus pole“. Potřebujeme ukázat, že pak lze dláždít i „čtverec 2^{n+1} minus pole“.

Postupujeme následovně. Šachovnici o straně 2^{n+1} (bez pole) rozdělíme na stejně velké čtvrtiny. Pak vyjmeme jedno trimino hned u středu tak, aby zmizela právě tři ze čtyř polí okolo středu, a to ta, která nejsou ve stejné čtvrtině jako to chybějící pole. Tímto způsobíme, že teď v každé čtvrtině chybí jedno pole, a každá z těchto čtvrtin je čtverec o straně 2^n .

Podle indukčního předpokladu dokážeme každou z těchto čtvrtin pokrýt triminy, pak ještě doplníme jedno navíc do vynechaného středu a jsme hotovi, pokryli jsme čtverec o straně 2^{n+1} bez pole.

□



Praktické pokrytí konkrétní šachovnice můžeme udělat opakovanou aplikací rekurzivního kroku, tedy opakovaným čtvrcením, dokud nedojdeme k velikosti 2×2 , a pak následným zpětným chodem. Mimochodem, dobrá otázka: Kolik je pro dané n potřeba trimin? Pokud tento počet označíme jako t_n , pak nám naše dekompozice dává následující rovnici: $t_{n+1} = 4t_n + 1$. Jak vypadají první hodnoty? Pro šachovnici 2×2 stačí jedno, tedy $t_1 = 1$. Pak máme:

$$\begin{aligned}t_1 &= 1, \\t_2 &= 4 \cdot 1 + 1, \\t_3 &= 4(4 \cdot 1 + 1) + 1 = 4^2 + 4 + 1, \\t_4 &= 4(4^2 + 4 + 1) + 1 = 4^3 + 4^2 + 4 + 1, \dots\end{aligned}$$

Tipujeme, že $t_n = 4^{n-1} + 4^{n-2} + \dots + 4^1 + 4^0$ a pro součet geometrické posloupnosti máme vzorec.

$$t_n = \sum_{k=0}^{n-1} 4^k = \frac{1-4^n}{1-4} = \frac{1}{3}(4^n - 1).$$

Ověření správnosti tohoto vzorce indukcí necháme na čtenáři, viz kapitola 10.

△

Příklad 7e.b: Uvažujme turnaj, jehož účastníci hrají každý s každým. Pro zjednodušení budeme předpokládat, že každý s každým hraje pouze jednou, a budeme značit $x \succ y$ fakt, že hráč x porazil hráče y (nehrajeme na remízy). Jak jsme poznamenali v kapitole 6, nedá se čekat, že by tato relace dala uspořádání, protože se často vyskytují cykly.

Připomeňme, že cyklem délky n (pro $n \geq 2$) rozumíme situaci, kdy máme hráče h_1, h_2, \dots, h_n takové, že $h_1 \succ h_2 \succ \dots \succ h_n$ a $h_n \succ h_1$. (Na něčem podobném je založena známá skautská desková hra, kdy slon pobije tygra, tygr vlka, vlk psa, pes kočku, kočka myš, ale myš zažene slona).

Protože každá dvojice h_1, h_2 spolu hraje jen jednou, není možné mít $h_1 \succ h_2$ a $h_2 \succ h_1$, tedy není možné mít cyklus délky 2, jen delší.

Dokážeme indukcí na délku cyklu, že jestliže se ve výsledcích turnaje najde cyklus, pak se v něm najde i cyklus délky 3.

(0) $n = 3$: triviální, už máme cyklus délky 3.

(1) Mějme libovolné $n \geq 3$. Předpokládejme, že každý turnaj s cyklem délky n má podcyklus délky 3. Chceme ukázat, že podcykly délky 3 mají i všechny turnaje s cyklem délky $n + 1$.

Uvažujme proto nějaký cyklus $h_1 \succ h_2 \succ \dots \succ h_n \succ h_{n+1} \succ h_1$. Podívejme se na dvojici h_1, h_3 .

Jestliže $h_3 \succ h_1$, tak máme 3-cyklus $h_1 \succ h_2 \succ h_3 \succ h_1$ a je hotovo.

Jestliže naopak $h_1 \succ h_3$, tak lze h_2 z původního cyklu vynechat a dostaneme nový cyklus délky n $h_1 \succ h_3 \succ h_4 \succ \dots \succ h_n \succ h_{n+1} \succ h_1$, v něm podle indukčního předpokladu umíme najít 3-cyklus.

□

Právě jsme viděli aplikaci indukce v oblasti zvané teorie grafů, viz kapitola 12.

△

Příklad 7e.c: Ukážeme aplikaci z teorie her.

Mějme dvě hromádky zápalek a dva hráče. Ti se střídají, v každém tahu si hráč vybere jednu hromádku a z ní pak odebere alespoň jednu zápalku. Hráč, který vezme poslední zápalku, vyhraje.

Ukážeme, že pokud je na začátku v obou hromádkách stejně zápalek, tak má druhý hráč výherní strategii (tedy algoritmus, který vede vždy na výhru, ať už dělá první hráč cokoliv).

Dále ukážeme, že pokud se počet zápalek v hromádkách různí, tak má první hráč výherní strategii.

Poznámka: Je to tedy jedna z her, u které je již na začátku rozhodnuto, jak to dopadne, pokud hráči hrají alespoň trochu inteligentně. Kupodivu i takové hry se hrají, například v Severní Americe tolik populární piškvorky na čtverci 3×3 zvané tic-tac-toe.

1) Nejprve dokážeme silnou indukci pro $n \geq 1$: Pokud je na začátku v obou hromádkách n zápalek, pak má druhý hráč výherní strategii.

(0) $n = 1$: První hráč musí vzít jednu zápalku, nemůže vzít obě (jsou na různých hromádkách), druhý pak vezme druhou neboli poslední a vyhrál.

(1) Nechť $n \geq 1$. Předpokládejme, že druhý hráč má výherní strategii pro všechny hry, ve kterých je na začátku na obou hromádkách stejně zápalek, a to nejvýše n . Chceme ukázat, že pak má výherní strategii také pro situaci s $n + 1$ zápalkami na obou hromádkách.

Takže máme dvě hromádky po $n + 1$ zápalkách. Nechme udělat prvního hráče první tah, odebere $r \geq 1$ zápalek z jedné hromádky. Pokud $r = n + 1$, tak už vzal všechny, druhý hráč odebere druhou hromádku a vyhrál. Pokud

$r < n + 1$, tak v první hromádce zbylo $n + 1 - r$ zápalek, druhý hráč pak na to reaguje tak, že odebere r zápalek z hromádky druhé. Teď je v obou hromádkách $n + 1 - r$ zápalek a je na tahu první hráč, čili jakoby hra začínala znovu, a protože obě hromádky mají po $n + 1 - r$ zápalkách, kde $1 \leq n + 1 - r \leq n$, má podle indukčního předpokladu druhý hráč výherní strategii.

Tím je dokázán indukční krok (1), spolu s (0) to potvrzuje existenci výherní strategie pro druhého hráče.

□

2) Pokud není na hromádkách stejně, tak první hráč prvním tahem odebere z větší hromádky tolik, aby srovnal počty. Teď je na obou hromádkách stejně a druhý hráč jakoby začíná, čímž se role prohodily a první hráč má výherní strategii.

Jako obvykle nám naše důkazy zároveň daly algoritmus k řešení problému, v tomto případě strategii pro výhru. Pokud může, hráč prostě vždy dorovnává hromádky na stejný počet a nakonec vyhraje.

Teorie her je zajímavá oblast matematiky s aplikacemi v mnoha oborech, u některých to nepřekvapí (ekonomie, diplomacie, vojenské vědy), u některých možná ano (genetika).

△

Nerutinní situace někdy bývají u indukce zrádné, protože chyba se dá udělat nejen ve struktuře, ale také je možné přehlédnout zádrhel při přechodu mezi případy n a $n + 1$.

Příklad 7e.d: „Dokážeme“ indukci, že v každé (neprázdné) třídě jsou vždy všichni studenti stejní.

(0) Příklad $n = 1$ je zřejmý, ve třídě s 1 studentem to platí.

(1) Nechť $n \in \mathbb{N}$ je libovolné. Předpokládejme, že stejnost studentů platí pro všechny třídy s n studenty. Teď mějme nějakou třídu T s $n + 1$ studenty. Zvolme nějakého studenta $a \in T$ a uvažujme třídu $A = T \setminus \{a\}$. Tato má n studentů, tudíž podle indukčního předpokladu jsou v ní všichni stejní. Zbývá ukázat, že i a musí být stejný jako ostatní studenti z A . Protože $n + 1 \geq 2$, lze najít $b \in T$ takové, že $b \neq a$. Uvažujme třídu $B = T \setminus \{b\}$. I ta má n studentů, i v této třídě musí být všichni stejní.

Teď zvolme nějaké $c \in T \setminus \{a, b\}$, čili studenta, který je v A i v B . Protože $c \in A$, jsou všichni z A stejní jako c ; protože také $c \in B$, jsou všichni z B stejní jako c . A protože $T = A \cup B$, jsou všichni z T stejní jako c neboli jsou všichni stejní.

Důkaz je hotov.

Kde je chyba? Rozhodně ne v indukci, struktura důkazu je zcela správně. Problémy musíme hledat v jednotlivých argumentech. První odstavec části (1) je správně, tomu není co vytknout. Problém je v druhém odstavci: Jak víme, že se takové c dá najít? Kdyby $T = \{a, b\}$, pak žádné c není, tudíž celý důkaz padá. Z toho je vidět, že implikace $V(n) \implies V(n + 1)$ platí pro všechna $n \geq 2$, ale neplatí pro $n = 1$ a to už stačí, aby celý důkaz indukci neplatil.

Zároveň se tím ukazuje, proč v matematice vyžadujeme, aby byl každý krok v důkazu opravdu něčím podepřen. Když matematik v onom důkazu čte „zvolme nějaké c “, tak se okamžitě ptá: Opravdu můžeme? Chrání se tím před chybami z přehlédnutí. Matematici jsou detailisti z nutnosti, nikoliv dobrovolně.

△

Příklad 7e.e: „Dokážeme“ indukci, že pro všechna $x, y \in \mathbb{N}$ platí $x = y$ (tedy všechna přirozená čísla jsou si rovna).

Použijeme indukci podle toho, jak jsou x a y velká, což nám říká hodnota $\max(x, y)$. Tu tedy použijeme v indukci jako krokovací parametr. Formálně:

Pro $n \in \mathbb{N}$ dokážeme: Jestliže $x, y \in \mathbb{N}$ a $\max(x, y) = n$, pak $x = y$.

(0) Jestliže $x, y \in \mathbb{N}$ a $\max(x, y) = 1$, pak $1 \leq x \leq 1$ a $1 \leq y \leq 1$, tedy opravdu $x = 1 = y$.

(1) Předpokládejme, že pro jisté (libovolné) $n \in \mathbb{N}$ platí $V(n)$, potřebujeme ukázat, že platí také $V(n + 1)$. Mějme tedy nějaké $x, y \in \mathbb{N}$ takové, že $\max(x, y) = n + 1$. Pak $\max(x - 1, y - 1) = n$, tudíž dle indukčního předpokladu $x - 1 = y - 1$, proto $x = y$. Důkaz je hotov.

Kde je chyba tady? Tu často odhalíme, když nějaký podezřelý případ zkusíme projet rekurzivním algoritmem, který je vlastně v indukci schovaný. Jak třeba ukážeme, že $2 = 4$? Máme $\max(2, 4) = 4$, podle indukčního kroku se pak odvoláváme na případ $\max(1, 3) = 3$, z toho zase na případ $\max(0, 2) = 2$ a hned máme problém, protože náš postup s nulou nepočítal. Kde je tento problém schován v našem „důkazu“? Právě provedený zpětný chod naznačuje, že je to někde v aplikaci indukčního předpokladu. Pokud chceme v důkazu něco použít, musíme hlídat, zda ona věc nemá nějaké zabudované podmínky. U indukčního předpokladu to vždy bývá to, že jej můžeme použít jen pro naše konkrétní n , ale už ne pro jiná čísla. Někdy má ale indukční předpoklad zabudovány další podmínky. Projdeme to v našem příkladě.

Používáme jej se zvoleným n , to je v pořádku. Pak je tam ovšem omezení, na které páry čísel jej můžeme aplikovat. Je dvojice $x - 1, y - 1$ v pořádku? Určitě platí $\max(x - 1, y - 1) = n$, to je základní algebra, takže tato

podmínka je v pořádku. Pak je tam ale ještě jedna věc: máme mít $x - 1 \in \mathbb{N}$ a $y - 1 \in \mathbb{N}$. A jak jsme viděli, v tom je právě zádrhel. Pro $x = 1$, popř. $y = 1$ se dostaneme k nule, která už není v \mathbb{N} a indukční předpoklad nejde použít. Tím je celý důkaz špatně.

△

Jako domácí úkol matematickou indukcí dokažte, že do autobusu jezdícího z kolejí do školy se vejde libovolný počet lidí.

Příklad 7e.f: Tento problém je znám po názvem Hanojské věže. Představte si tři tyčky, na jedné je navlečeno n disků (s dírkou uprostřed) pěkně podle velikosti od největšího dole po nejmenší nahoře. (Chtěl jsem udělat obrázek, ale místo toho vás pošlu do nejbližšího hračkářství, kde v oddělení pro mrňata určitě tyčku s kolečky mají.) Cílem je dostat tyto disky do stejné pozice, ale na jiné tyčce, pomocí série tahů. Tah funguje takto: Vybereme disk, který je na některé z tyčí nahoře, a přeneseme jej buď na prázdnou tyč nebo na jiný disk, který leží nahoře a je větší než ten, který přesouváme.

V průběhu řešení se tak disky přesouvají a vytvářejí na tyčích „pyramidy“, protože se podle pravidel nikdy nemůže stát, že by větší disk ležel na menším. V libovolném okamžiku tedy na každé tyči budou disky v pořadí od největšího dole po nejmenší nahoře. Pokud prohlásíme i prázdnou tyč za pyramidu, tak povoleným tahem je přenést jeden disk z vrcholu jedné pyramidy na jinou.

Je možné tuto úlohu vyřešit?

Ať už vymyslíme jakýkoliv způsob, nakonec musí přijít okamžik, kdy přesouváme dolní, největší disk na cílovou tyč. Abychom to mohli udělat, je nutné všechny disky nad ním dát někam jinam, ale žádný z nich nesmí přijít na cílovou tyč, to bychom totiž ten největší nemohli dát na něj; konec konců, my ten největší stejně chceme dát až dolů. Vidíme tedy, že nutnou přípravou pro přesunutí největšího disku je, aby všechny ostatní byly na té třetí tyči, a to samozřejmě podle velikosti (jinak to nejde). Shrnutí, chceme-li přenést celou pyramidu řekněme na tyč 2, musíme tam dát dolů největší disk, což vyžaduje přenesení pyramidy disků nad ním na tyč číslo 3.

Dostáváme tím jasnou rekurzi. Začneme s pyramidou n disků na tyči 1, a abychom ji přenesli na tyč 2, musíme nejprve přenést horních $n - 1$ disků na tyč 3. Tuto menší pyramidku o $n - 1$ discích přeneseme tak, že její největší disk chceme přenést na cílovou tyč 3, ale na to potřebujeme to, co je nad ním, tedy pyramidku velikosti $n - 2$, přenést na tyč 1 či 2 atd. Dříve či později dojdeme k tomu, že máme někam přenést jeden disk, a to ten nejmenší, což lze bez problémů.

Proveditelnost by tedy mělo jít dokázat indukcí. Jediná trochu nejasná věc je, že uprostřed řešení budeme v situaci, kdy máme přenést řekněme pyramidu s 13 disky, ale dalších 5 disků z předchozího rekurzivního rozkladu už se někde potuluje. Nedojde při pokusu o skutečnou realizaci našeho algoritmu ke konfliktu s pravidly? Naštěstí ne. Všechny ty disky z předchozího rozkladu jsou totiž větší než ty v naší pyramidě, tudíž je můžeme v dané chvíli považovat za podlahu; v přesouvání té pyramidy nás neomezí. Raději to zapracujeme do našeho důkazu.

Zkusíme tedy dokázat indukcí, že dokážeme přenést pyramidu n disků z libovolné tyče a na libovolnou jinou tyč b , přičemž na tyčích (i pod pyramidou) již mohou být dole nějaké větší disky.

(0) $n = 1$: Jeden disk určitě přeneseme na cílovou tyč, přičemž nám nebude vadit, když už tam bude nějaký větší disk.

(1) Předpokládáme, že pyramidu o velikosti n umíme. Mějme pyramidu o $n + 1$ discích na tyči a (pod kterou mohou být větší disky), potřebujeme ji dostat na tyč b , přičemž na tyčích b a c už jsou třeba nějaké disky větší než ty v naší pyramidě. Nejprve použijeme indukční předpoklad a přesuneme horních n disků naší pyramidy na tyč c (v tom nám případný větší disk dole nebude vadit), pak přesuneme spodní disk naší pyramidy na tyč b (ani v tom nám případný větší disk nebude vadit), načež opět využijeme indukční předpoklad a přesuneme horních n disků naší pyramidy z tyče c na tyč b , kde už leží disk s číslem $n + 1$, který je větší než disky pyramidky nad ním, i to je v pořádku.

Tím je důkaz hotov.

To bylo snadné. Mnohem zajímavější je otázka, kolik přesunů disků („tahů“) na to budeme potřebovat. Označme jako H_n počet tahů, které náš algoritmus spotřebuje na přesun pyramidy o n discích. Je jasné, že $H_1 = 1$. Postup v kroku (1) pak říká, že $H_{n+1} = H_n + 1 + H_n = 2H_n + 1$.

Jde o klasickou rekurentní definici posloupnosti. K jejímu určení použijeme trochu optimismu a Větu 8c.5.

$$\begin{aligned} H_n &= 2H_{n-1} + 1 = 2(2H_{n-2} + 1) + 1 = 2^2H_{n-2} + 2 + 1 \\ &= 2^2(2H_{n-3} + 1) + 2 + 1 = 2^3H_{n-3} + 2^2 + 2 + 1 \\ &= 2^3(2H_{n-4} + 1) + 2^2 + 2 + 1 = 2^4H_{n-4} + 2^3 + 2^2 + 2 + 1 = \dots \\ \dots &= 2^{n-1}H_1 + 2^{n-2} + \dots + 2^2 + 2 + 1 = \sum_{k=0}^{n-1} 2^k = \frac{1-2^n}{1-2} = 2^n - 1. \end{aligned}$$

Dokažte, že $G(n) \leq 2n - 4$ pro všechna $n \geq 4$.

Poznámka: Dá se ukázat, že ve skutečnosti je tam rovnost, není možné to provést za méně než těch $2n - 4$ hovorů. To už je ale těžký problém.

Řešení:

7e.1: $V(n)$: Jestliže je $4n + 1$ zápalek, tak má druhý hráč výherní strategii.

(0) $n = 0$: Je jedna zápalka, zbyla na prvního hráče, ten prohrál.

(1) $n \geq 0$: IP: Druhý hráč umí vyhrát hru s $4n + 1$ zápalkami. Uvažujme hru s $4(n + 1) + 1 = 4n + 5$ zápalkami. První hráč vezme zápalky, povolený počet je 1, 2, 3. Cokoliv vezme, druhý hráč může vždy vzít tak, aby zbylo $4n + 1$ zápalek a je na tahu první, tedy hra znovu začíná s $4n + 1$ zápalkami a druhý má výherní strategii.

Důkaz, že jinak má výherní strategii první hráč: Jestliže je počet zápalek $4n + 2$, $4n + 3$ nebo $4n + 4$, tak první hráč odebere tak, aby zbylo $4n + 1$ a je na tahu druhý hráč. Začíná hra s $4n + 1$ zápalkami, ve které původně první hráč hraje roli druhého a má výherní strategii.

7e.2: 1) Indukcí: (0) $n = 4$: $G(4) = 4 \leq 2 \cdot 4 - 4$. (1) $n \geq 4$: IP: $G(n) \leq 2n - 4$. Teď uvažujme $n + 1$ osob. Jedna z nich někomu ze skupiny řekne svou informaci. Pak se odpojí, zbývajících skupině o n lidech stačí $G(n)$ hovorů k tomu, aby v ní už všichni věděli všechno, včetně informace první osoby. Podle indukčního předpokladu na to stačí $2n - 4$ hovorů. Pak někdo ze skupiny ještě řekne všechny informace té první osobě. Celkem stačí $1 + (2n - 4) + 1 = 2n - 2$ hovorů. Nevíme ale, jestli zrovna tato strategie je optimální, takže je to horní odhad, máme tedy $G(n + 1) \leq 2n - 2 = 2(n + 1) - 4$.

2) Přímo: Pro $n = 4$ to platí. Nechtě $n \geq 5$. Označíme nějaké čtyři osoby jako 1,2,3,4. Všichni ostatní si promluví s někým z této čtveřice. Pak tedy tato čtveřice jako skupina ví všechno.

Pak si informace navzájem vymění, na to stačí čtyři rozhovory 1-2, 3-4, 1-3, 2-4, tím každý ze skupiny ví všechno. Nakonec třeba 1 promluví s těmi $n - 4$ mimo skupinu. Celkem tedy stačí $(n - 4) + 4 + (n - 4) = 2n - 4$ hovorů.

Poznámka: Kolik by bylo třeba hovorů, kdyby všech $n - 1$ řeklo svou informaci člověku 1, ten pak zná vše, tak to řekne ostatním?

Kolik by bylo třeba hovorů, kdyby v té speciální skupině byli 2, popřípadě 3 lidi? A pět lidí?