5. Indukce a rekurze

Na matematickou indukci jsme již v této knize několikrát narazili v důkazech. Je obtížné si představit matematiku bez tohoto silného nástroje, který si v této kapitole oficiálně představíme. Začneme oním jednoduchým typem důkazu indukcí, který už mnozí z čtenářů znají a který jsme zatím používali, a postupně se propracujeme k složitějším verzím, protože indukce znamená víc, než asi čtenář dosud tušil.

5a. Matematická indukce

Když student slyší „matematická indukce“, obvykle si představí důkaz, kterým ukazujeme pravdivost rozličných vzorečků. Začneme tím, že si přesně formulujeme, jak vlastně takový důkaz funguje.

! **5a.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 jsou splněny následující předpoklady:
(0) $V(n_0)$ platí.
(1) Pro každé $n \in \mathbb{Z}$, $n \geq n_0$ je pravdivá následující implikace: Jestliže platí $V(n)$, pak platí i $V(n+1)$.
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 $n \geq n_0$ 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.

Pokud tedy chceme dokázat univerzální platnost nějaké vlastnosti V, stačí dokázat pravdivost tvrzení (0) a (1). Proč to stačí? Půjčíme si představu žebříku. Tzv. **základní krok** (0) říká, že umíme vylézt na první příčku žebříku. Tzv. **indukční krok** (1) říká, že když už někde jsme, tak umíme vylézt o příčku výš. Podstatný je ten obecný kvantifikátor v (1), indukční krok je splněn pro libovolné místo na žebříku. Selský rozum říká, že pak už se dostaneme na žebříku všude.

Zkusme to matematicky, vezmeme pro jednoduchost $n_0 = 1$. Podle základního kroku platí $V(1)$. Indukční krok dává pro volbu $n = 1$ pravdivou implikaci $V(1) \implies V(2)$, my už ovšem ze základního kroku víme, že $V(1)$ platí, tudíž podle této implikace platí i $V(2)$. Pak zase můžeme použít indukční krok s $n = 2$, kde z pravdivosti $V(2)$ dostaneme pravdivost $V(3)$. Další použití indukčního kroku (s $n = 3$) dá pravdivost $V(4)$, pak $V(5)$ a tak dále. Člověk by si řekl, že se tohle nemůže pokazit, dojdeme takto libovolně daleko a V funguje pro všechna čísla. Princip výše potvrzuje, že tato představa je správná.

Jiná dobrá představa je padající domina. (1) říká, že kdykoliv nějaké domino spadne, tak spadne i to další. (0) říká, že jsme shodili to první. Zkušenost říká, že pak by to mělo spadnout všechno. Zároveň vidíme, že nic nelze vynechat. Pokud nedokážeme (0), tak vlastně na začátku nic neshodíme a domina nepadají. Pokud není pravda, že (1) platí pro všechna relevantní n, tak se pro některé n padání domina zadrhne.

! **Příklad 5a.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. Jaké jsou jednotlivé kroky?

• *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.
Zde je dobré si rozmyslet, že $1 + 3 + \cdots + (2n-1)$ *opravdu dává prvních n lichých (kladných) čísel.*
• *Dokážeme základní krok.*
(0) Nechť $n = 1$. Vlastnost $V(1)$ zní $1 = 1$, 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* $V(n+1)$*. Základním trikem je při tom dekompozice, kdy se* $V(n+1)$ *pokusíme rozložit tak, aby se objevilo něco, na co lze aplikovat* $V(n)$*.*
(1) Nechť $n \in \mathbb{N}$ je libovolné. Předpokládejme, že $1 + 3 + 5 + \cdots + (2n-1) = n^2$.

Chceme pomocí této rovnosti nějak ukázat, že pro naše konkrétní n platí také $1+3+5+\cdots+(2(n+1)-1) = (n+1)^2$, *tedy že* $1+3+5+\cdots+(2n+1) = (n+1)^2$. *Obvykle bývá lepší začít tou delší či více komplikovanou stranou a upravit ji tak, aby se objevilo něco, co je i ve* $V(n)$, *pomocí tohoto předpokladu se pak propracujeme ke druhé straně ve* $V(n+1)$.

Zde je to snadné, dokazovaná rovnost obsahuje $1+2+\cdots+(2n-1)$. *Jdeme na to.*

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

• *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 i u dalších důkazů zachováváme tuto strukturu.

△

S 5a.2 Poznámka: Začínající studenti jsou zvyklí dokazovat neznámé rovnosti tak, že si je napíší a pak upravují, dokud nedostanou něco známého. U předchozího příkladu by například napsali

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

Bohužel, toto není důkaz platnosti $V(n+1)$, ale důkaz platnosti rovnosti $0=0$, jde totiž špatným směrem. Navíc ani nejde o důkaz korektní, vychází totiž z rovnosti, jejíž platnost v té chvíli není známá. Správný důkaz samozřejmě vychází z něčeho, co je známé, a dojde k tomu, co chceme dokázat. V tomto případě vznikne správný důkaz tak, že ty řádky znovu přepíšeme, ale v opačném pořadí. Při tom přepisování ale musíme pečlivě hlídat, zda kroky, které jsme předtím dělali, platí i v opačném „správném“ směru. U tohoto příkladu to platí, neboť všechny provedené úpravy byly ekvivalentní, ale ne vždy tomu tak je.

I v případě, že kroky obrátit jdou, jde o zbytečnou komplikaci, mnohem kratší je dokázat zadanou rovnost přímým výpočtem, tedy začít výrazem na jedné straně a postupně se propracovat k výrazu na druhé straně, přesně jak jsme to udělali v příkladě 5a.a. Nejen že je to kratší, zejména u nerovností jde často o jediný rozumný přístup (viz příklad 5a.e a poznámka 5a.4), proto jej doporučujeme.

Podrobněji o tomto problému pojednává poznámka 1b.6.

△

Příklad 5a.b: Než začneme, tak si rozmyslíme, že čísla typu 11, 1001, 100001, ... se dají zapsat způsobem $10^{2n+1}+1$ pro $n \in \mathbb{N}_0$. Číslo n nám vlastně říká, kolik dvojic 00 je uprostřed.

Dokážeme pro $n \in \mathbb{N}_0$ toto $V(n)$: Číslo $10^{2n+1}+1$ je dělitelné 11.

Připomeňme, že to vlastně znamená následující: Číslo $10^{2n+1}+1$ lze zapsat jako $11k$ pro nějaké celé číslo k.

(0) Pro $n=0$ to platí: $10^1+1 = 11 = 11\cdot 1$.

(1) Mějme libovolné $n \geq 0$, předpokládejme platnost $V(n)$, tedy že $10^{2n+1}+1 = 11k$ pro nějaké $k \in \mathbb{N}$. Potřebujeme ukázat platnost $V(n+1)$, tedy že i číslo $10^{2(n+1)+1}+1 = 10^{2n+3}+1$ je násobkem 11. Abychom mohli využít indukční předpoklad, musíme si nejprve v tomto čísle najít číslo z $V(n)$ chytrým přepsáním. Máme $10^{2n+3}+1 = 10^{2n+1+2}+1 = 100\cdot 10^{2n+1}+1$, ještě potřebujeme přidat na správné místo $+1$, což uděláme oblíbeným trikem, že si to přidáme tam, kde to chceme mít, ale pak to musíme také odebrat. Po malé úpravě pak už můžeme použít indukční předpoklad.

$$10^{2n+3}+1 = 100\cdot(10^{2n+1}+1-1)+1 = 100\cdot(10^{2n+1}+1)-100+1 = 100\cdot 11k-99 = 11(100k-9),$$

kde číslo $100k-9$ je celé. Odvodili jsme, že $10^{2(n+1)+1}+1$ je násobek 11 a tedy $V(n+1)$ platí. Důkaz je hotov.

Alternativa při dekompozici je, že si nejprve upravíme vztah z $V(n)$ na $10^{2n+1} = 11k-1$ a pak už stačí si ve výrazu z $V(n+1)$ vyrobit 10^{2n+1}, což jsme snadno udělali výše. Nakonec to vyjde nastejno.

△

Matematická indukce je mocný nástroj, který lze aplikovat i na jiné situace než dokazování vzorečků. Zhruba řečeno, o indukci začínáme přemýšlet, když zkoumáme situaci, kterou lze rozložit do etap, ve kterých se nějak přirozeně vyskytuje parametr n coby přirozené číslo, a existuje nějaký vztah mezi etapou současnou a následnou,

či jinak řečeno mezi současnou a tou předchozí (záleží, jak v dané chvíli zrovna přemýšlíme, zda dopředu nebo se vracíme do minulosti).

Příklad 5a.c: 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.

Když se hry dohrají, rádi bychom srovnali hráče podle výkonnosti. To se obvykle dělá podle bodů, protože dělat rozumné pořadí jen na základě výsledků je nemožné. Jedním z možných problémů jsou tzv. cykly, nelze rozumně uspořádat tři hráče podle výkonnosti, pokud první porazil druhého, ten třetího, ale třetí zase porazil prvního. Obecněji, cyklem délky n rozumíme situaci, kdy máme hráče $h_1, \ldots, h_n$ takové, že $h_1 \succ h_2 \succ \cdots \succ h_n$, ale $h_n \succ h_1$. (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).

Dokážeme indukcí vlastnost $V(n)$: Jestliže se ve výsledcích turnaje najde cyklus délky n, pak se tam najde i cyklus délky 3.

Tato vlastnost má smysl jen pro $n \geq 3$, protože ze dvou (a méně) hráčů cyklus při vší snaze nevyrobíme.

(0) $n = 3$: triviální, už máme cyklus délky 3.

(1) Mějme libovolné $n \in \mathbb{N}$, $n \geq 3$. Předpokládejme platnost $V(n)$, zajímá nás platnost $V(n+1)$. Uvažujme proto nějaký cyklus $h_1 \succ h_2 \succ \cdots \succ h_n \succ h_{n+1}$, kde také $h_{n+1} \succ h_1$. Potřebujeme se nějak dostat k indukčnímu předpokladu, tedy k cyklu délky n. To se dělá tak, že se zeptáme, jak dopadl souboj h_1 a h_3. Jestliže $h_3 \succ h_1$, tak máme 3-cyklus $h_1 \succ h_2 \succ h_3$ a je hotovo.

Jestliže naopak $h_1 \succ h_3$, tak lze h_2 z původního cyklu vynechat a dostaneme nově cyklus délky n $h_1 \succ h_3 \succ h_4 \succ \cdots \succ h_n \succ h_{n+1}$, v něm podle indukčního předpokladu umíme najít 3-cyklus. Tím je důkaz (1) hotov.

Podle (0) a (1) platí $V(n)$ pro všechna $n \geq 3$.

Právě jsme viděli aplikaci indukce v oblasti zvané teorie grafů.

△

! **Poznámka:** Všimněte si jednoho důležitého momentu. Oficiálně se indukce tváří, že v ní jde o „krok nahoru". Známe současnost a ptáme se, zda pomocí ní dokážeme také zvládnout další etapu. Když ji ale vymýšlíme, tak nás často zajímá opačná otázka: „Pokouším se vyřešit úlohu na nějaké úrovni. Pomohlo by mi, pokud bych věděl, že tu úlohu umím rozřešit o úroveň níže?" Jestliže si na tuto otázku odpovím kladně a vymyslím způsob, jak vyřešit daný problém za předpokladu, že znám řešení předchozí situace, tak jsem zároveň přišel na způsob, jak provést důkaz v (1). Jde tedy o rekurzivní způsob přemýšlení, indukce a rekurze jsou tak propojeny, že je těžké rozlišit, kde jedna končí a druhá začíná.

Funguje to i naopak. Pokud najdeme důkaz (1), tak se obvykle stává návodem, jak vytvořit algoritmus k praktickému řešení studovaného problému, od indukčního důkazu bývá tedy jen krůček k rekurzivnímu algoritmu.

△

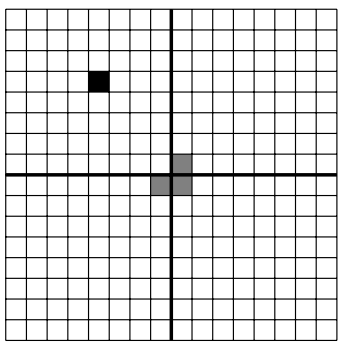
Příklad 5a.d: Uvažujme čtvercovou šachovnici se stranou o velikosti 2^n polí. (Jinak řečeno, uvažujme čtverec zformovaný z $(2^n)^2$ malých čtverců, kde $n \in \mathbb{N}$.) Začerněme jedno z polí. Tvrdíme, že to, co zbyde, lze zcela pokrýt dlaždicemi složenými ze 3 čtverečků ve tvaru L (tzv. trimin, viz obrázek) tak, aby se nepřekrývaly.

Chceme dokázat $V(n)$: Popsané pokrytí je možné pro čtverec o straně 2^n bez jednoho pole. 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 mínus pole". Potřebujeme ukázat, že pak lze dláždit i „čtverec 2^{n+1} mínus 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 těch 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.

Důkaz je hotov.

Praktické pokrytí konkrétní šachovnice můžeme udělat opakovanou aplikací rekurzivního kroku $V(n+1) \mapsto V(n)$, 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: $t_{n+1} = 4t_n + 1$. Takovéto rovnice se naučíme řešit v kapitole o rekurentních rovnicích, viz příklad .

△

S 5a.3 Poznámka (a velice důležitá!): Pro správné chápání indukce je kritické si uvědomit, že jsme v příkladech nikdy přímo nedokazovali, že by $V(n)$ platilo. Sice se tam říkalo „předpokládejme, že $V(n)$ platí," ale to byl jen předpoklad dokazované implikace, který může a nemusí být pravda. Také jsme v důkazu řekli slova „$V(n+1)$ platí," ale to bylo pouze za předpokladu, že platí i $V(n)$. Je veliký rozdíl mezi tvrzením „$V(n+1)$ platí" a tvrzením „$V(n+1)$ platí, pokud platí i $V(n)$". Z druhého totiž o pravdivosti $V(n)$ či $V(n+1)$ samotných nic nevyplývá, jen že jsou jejich pravdivosti nějak svázány. V kroku (1) tedy dokazujeme, že se pravdivost přenáší z $V(n)$ na $V(n+1)$, *pokud tam nějaká je*. Chcete vidět příklad?

Uvažujme vlastnost $V(n)$: $n > 13$. Tvrdíme, že pro všechna $n \in \mathbb{N}$ platí následující implikace:

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

Důkaz je snadný. Vezměme si nějaké $n \in \mathbb{N}$. Jestliže platí předpoklad $n > 13$, pak také $n+1 > 13+1 = 14$, tedy platí i $n+1 > 13$.

Takže vidíme, že implikace $V(n) \implies V(n+1)$ platí pro všechna $n \in \mathbb{N}$, ale určitě není pravda, že by $n > 13$ pro přirozená čísla. Finta je v tom, že třeba $n = 2$ nesplňuje $V(2)$, tudíž nám (pravdivá) implikace $V(2) \implies V(3)$ neřekne vůbec nic o pravdivosti $V(3)$.

K důkazu vlastnosti V tedy pravdivost (1) sama o sobě nestačí, to jsme jen postavili domina jedno za druhé. Teprve když doplníme kritický krok (0), tedy šťouchneme do prvního, tak se celá mašinerie rozběhne a pomocí (1) už tato pravdivost dojede libovolně daleko čili všude. U našeho příkladu se to povede, když dokážeme (0): Číslo $n = 14$ splňuje $n > 13$. Tím se proces nastartuje a vlastnost V pak už platí pro všechna $n \geq 14$. K tomuto tématu se vrátíme v poznámce 5a.5.

Využijme této situace k diskusi dalšího problému, který studenti s indukcí mívají. Často zapomenou v kroku (1) napsat kvantifikátor, tedy namísto správného $\forall n$: $[V(n) \implies V(n+1)]$ dokazují jen $V(n) \implies V(n+1)$. Není pak jasné, co tím vlastně myslí.

Ještě horší je, pokud ten kvantifikátor špatně umístí. Někdy začnou důkaz části (1) takto: „Předpokládejme, že pro všechna n platí $V(n)$." Dokazují pak implikaci $[\forall n\colon V(n)] \implies V(n+1)$, která jednak není formálně správně (jaké n se bere ve vlastnosti $V(n+1)$?), navíc to ani nedává smysl, protože v zásadě není co dokazovat. Jestliže předpokládáme, že V platí pro všechna čísla, pak samozřejmě musí platit pro $n+1$. Pokud budeme předpokládat, že všichni lidé mají hranaté hlavy, pak automaticky má hranatou hlavu i Habala. Takováto implikace je tedy tautologií, platí vždy bez ohledu na to, jaká je vlastně vlastnost V.

Z pohledu indukce je ovšem daleko závažnější, že tato implikace je na nic. Potřebujeme implikaci, která ze známé platnosti V pro jedno číslo dokáže tuto platnost posunout o krok dál. Předpokladem oné „zprzněné" implikace je ovšem výrok $\forall n$: $V(n)$, o jehož platnosti nevíme nic, přesně tohle naopak chceme dokázat. Taková implikace je proto zcela k ničemu.

Správný zápis důkazů není jen formalita, pomáhá nám to správně pochopit smysl toho, co se děje.

△

! Viděli jsme (a ještě uvidíme), že indukci lze použít i v „nematematických" situacích. Její speciální schopností je, že nám umožňuje pracovat s konečně mnoha objekty, ale nakonec z té práce získat informaci o nekonečné množině. Z toho ale také plyne omezení jejího pole působnosti, protože takto obsáhneme jen věci očíslovatelné, jinými slovy situace spočetné. Jakmile máme nespočetnou situaci, tak je zbytečné o indukci uvažovat, do tak velkých množin ani pořádně nenakoukne.

Další problém je, že i situace spočetné ještě nemusí být zvládnutelné indukcí, protože sice očíslovatelné jsou, ale to číslování nemusí být v souladu s problémem, který chceme řešit, takže mezi případem s číslem n a případem s číslem $n+1$ nemusí být přímá souvislost. Tím ovšem padá naděje udělat indukční krok (1). Typické je to u racionálních čísel. Je pravda, že množinu $\mathbb{Q}$ jde očíslovat jak $\{r_n\}$, ale to číslování nemá žádnou rozumnou pravidelnost (že by třeba r_n šly podle velikosti či tak něco), proto se v $\mathbb{Q}$ s indukcí víceméně nepracuje. Ale dokonce i když číslování funguje rozumně a my vidíme cestu, jak jít od případu n k případu $n+1$, tak se může stát, že indukce selže, viz poznámka 5a.6.

Dosti zásadní problém u indukce je, že v okamžiku, kdy ji používáme, již musíme dopředu znát odpověď, kterou jsme museli získat nějak jinak. Klasický příklad je důkaz indukcí, že $1+2+\cdots+n = \frac{n(n+1)}{2}$, viz cvičení 5a.1 (ii), který je velice snadný, ale onen výraz na pravé straně se musel najít jinak, viz Fakt 9c.3 (ii) a obecnější trik v příkladě 10b.j.

Z pohledu studenta je velký problém indukce v tom, že vypadá tak snadno. U lehkých problémů tomu tak opravdu je, ale ve skutečnosti se v indukci skrývají kritická místa, která při zanedbání mohou pořádně potrápit. Začneme několika příklady s nerovnostmi, které studentům tradičně činí potíže.

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

(0) Jestliže $n = 3$, tak vlastnost $V(3)$ říká $3^2 > 8$, což určitě platí.

(1) Předpokládejme, že pro jisté libovolné $n \in \mathbb{N}$ splňující $n \geq 3$ máme $n^2 > n + 5$. Potřebujeme ukázat, že $(n+1)^2 > (n+1)+5$, tedy že $(n+1)^2 > n+6$. Použijeme doporučenou metodu, tedy začneme třeba levou stranou a zkusíme od ní dojít ke straně pravé, cestou někde použijeme indukční předpoklad. Na to si budeme muset v levé straně nějak vyrobit n^2, což lze například roznásobením té druhé mocniny.

$$(n+1)^2 = n^2 + 2n + 1 > (n+5) + 2n + 1 = n + 6 + 2n.$$

My se ale potřebujeme dostat k výrazu $n + 6$ a to takovým způsobem, abychom použili jen rovnost či nerovnosti $\geq$ a $>$. Zde je to naštěstí snadné, díky $n \geq 3$ určitě máme $2n \geq 0$, lze tedy ve výraze napravo $2n$ vynechat (či nahradit nulou, dívejte se na to, jak chcete) a tím jej zmenšit.

$$(n+1)^2 = n^2 + 2n + 1 > (n+5) + 2n + 1 = n + 6 + 2n \geq n + 6.$$

Opravdu jsme dostali, co bylo třeba, a důkaz je hotov.

Potvrdilo se, že u indukce s matematickými vzorečky se obvykle vyplatí začít s dekompozicí od komplikovanější části dokazovaného vztahu.

△

S 5a.4 Poznámka: Vracíme se k poznámce po prvním příkladu. I zde jsme při důkazu nerovnosti použili metodu postupných kroků. Začali jsme výrazem na jedné straně dokazovaného, pak jsme jej postupně upravovali a dospěli tak k žádanému. Všechny kroky byly aritmeticky v pořádku, v zásadě jsme používali následujícího prinicipu: Máme-li dvě čísla $a + b$ a teď jedno z nich nahradíme menším, třeba namísto a dáme menší c, pak je celek menší, tedy $a + b > c + b$. Podobně pokud máme $c \leq a$, pak po nahrazení dostaneme $a + b \geq c + b$. Tímto způsobem se nerovnosti v indukci dokazují docela spolehlivě, jen někdy dá trochu problém se strefit do cílového výrazu.

Naopak vůbec nefunguje ona populární metoda postupných úprav žádané nerovnosti. Zkusme si to pro náš příklad: Napíšeme žádanou nerovnost a zkusíme ji upravovat.

$$(n+1)^2 > n + 6$$
$$n^2 + 2n + 1 > n + 6.$$

A tím jsme skončili, indukční předpoklad sice říká, že $n^2 > n + 5$, ale my nemůžeme v naší nerovnosti nahradit část n^2 výrazem $n + 5$, protože to není korektní úprava! Jinými slovy, pokud by někdo jako další řádek napsal $n + 5 + 2n + 1 > n + 6$, tak by to měl špatně, podrobněji o tomto viz poznámka 1b.6. U nerovností tedy tento postup rozhodně nedoporučujeme. Pro další detaily viz poznámka 1b.6 a zejména příklad na konci kapitoly 14.

△

Příklad 5a.f: Dokážeme, že pro každé $n \in \mathbb{N}_0$ platí $V(n)$: $n < 2^n$.

(0) Nechť $n = 0$. Určitě $0 < 2^0$, tedy $V(0)$ platí.

(1) Předpokládejme, že pro jisté (libovolné) $n \in \mathbb{N}_0$ máme $n < 2^n$. Potřebujeme ukázat, že $n + 1 < 2^{n+1}$. Víme už, že postupné úpravy této nerovnice nefungují, musíme začít na jednom konci, třeba na pravém, a propracovat se k druhému. Nejprve potřebujme 2^{n+1} upravit tak, abychom mohli použít indukční hypotézu.

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

Teď se nějak potřebujem dostat dalšími úpravami k $n + 1$, a aby celý řetěz úprav platil, můžeme používat pouze kroky s rovností $=$ či nerovnostmi $\geq$ a $>$. Je vůbec možné se dostat od $2n$ k $n + 1$ tímto způsobem, jinými slovy, platí vůbec $2n \geq n + 1$? Ano, pokud $n \geq 1$, ale to my nemáme. Tím se ukazuje, že jsme svou indukci začali příliš brzy. Je sice pravda, že $V(0)$ platí, ale indukční krok $V(n) \implies V(n + 1)$ budeme umět dokázat až od $n = 1$. Začneme tedy s důkazem znovu, přičemž indukce začne až pro $n \geq 1$, případ $n = 0$ vyřešíme zvlášť.

Takže nejprve přímo ověříme, že $V(n)$ platí pro $n = 0$ (už jsme provedli výše). Teď pro $n \geq 1$ použijeme důkaz indukcí:

(0) $V(1)$ platí, určitě $1 < 2^1$.

(1) Předpokládejme, že pro jisté $n \in \mathbb{N}$ máme $n < 2^n$. Potřebujeme ukázat, že $n + 1 < 2^{n+1}$. Podle indukční hypotézy a z toho, že $n \geq 1$, dostaneme

$$2^{n+1} = 2 \cdot 2^n > 2 \cdot n = n + n \geq n + 1.$$

Důkaz je hotov.

△

5a.5 Poznámka:

Pro správné chápání indukce je třeba ocenit, že tvrzení (0) a (1) jsou nezávislé věci, každá si dělá něco jiného a jejich spojením pak teprve vznikne platný důkaz.

V příkladě 5a.e jsme měli situaci, kdy v (1) ten indukční krok $V(n) \implies V(n+1)$ platil pro všechna $n \geq 0$, ale nebylo nám to nic platné. Protože $V(0)$, $V(1)$ ani $V(2)$ neplatí, nešla tato implikace využít s malými čísly a běh indukce se dal začít až od $n = 3$.

Naopak v příkladě 5a.f jsme mohli v kroku (0) použít $n = 0$, ale nebylo to k ničemu, protože indukční krok $V(n) \implies V(n+1)$ se ruměl rozběhnout až pro vyšší n.

Pro další příklady podobného typu se podívejte na cvičení 5a.4 a 5a.5.

△

Indukce sice vypadá jako jednoduchá věc, ale pokud jí člověk dobře nerozumí, popřípadě pokud není dostatečně opatrný, může snadno udělat chybu.

! Příklad 5a.g: „Dokážeme“ indukcí, že v každé (neprázdné) třídě mají vždy všichni žáci stejné pohlaví (muž/žena).

Pro $n \in \mathbb{N}$ uvažujme $V(n)$: V každé třídě s n studenty mají všichni studenti stejné pohlaví.

(0) Případ $n = 1$ je zřejmý, ve třídě s 1 studentem to platí.

(1) Nechť $n \in \mathbb{N}$ je libovolné. Předpokládejme, že shoda pohlaví 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 $A = T - \{a\}$. Tato má n studentů, tudíž podle indukčního předpokladu mají všichni stejné pohlaví. Zbývá ukázat, že i a musí mít stejné pohlaví jako studenti z A. Protože $n + 1 \geq 2$, lze najít $b \in T$ takové, že $b \neq a$. Uvažujme třídu $B = T - \{b\}$. I ta má n studentů, i v této třídě musí mít všichni stejné pohlaví.

Teď zvolme nějaké $c \in T - \{a, b\}$, čili studenta, který je v A i v B. Protože $c \in A$, mají všichni z A stejné pohlaví jako c. Protože také $c \in B$, mají i všichni z B stejné pohlaví jako c. A protože $T = A \cup B$, mají všichni z T stejné pohlaví jako c. 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 indukcí 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.

△

! Příklad 5a.h: „Dokážeme“ indukcí, 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 $n \in \mathbb{N}$ uvažujeme $V(n)$: 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 i $V(n + 1)$. 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 si 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 si 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. Projděme si 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.

5a.6 Poznámka stranou: Někdy indukce narazí i v situaci, která na první pohled vypadá jako pro ni stvořená, rizikovým faktorem bývají nerovnosti. Ukážeme si to na následujícím příkladě: Zkusíme indukcí dokázat, že pro každé $n \in \mathbb{N}$ platí vlastnost $V(n)$: $\frac{n-1}{n} < 1$ (což je dozajista pravda).

(0) Pro $n = 1$ máme $V(1)$: $0 < 1$, což platí.

(1) Mějme libovolné $n \in \mathbb{N}$ a předpokládáme, že platí $\frac{n-1}{n} < 1$. Chceme dokázat, že pak platí i $V(n+1)$, tedy $\frac{n}{n+1} < 1$. Začneme s výrazem na levé straně, potřebujeme jej upravit tak, aby šlo použít indukční předpoklad.

$$\frac{n}{n+1} = \frac{n^2}{(n+1)(n-1)} \cdot \frac{n-1}{n} < \frac{n^2}{(n+1)(n-1)} = \frac{n^2}{n^2-1}.$$

A máme problém, rozhodně už se nám nepodaří tento řetězec výrazů zakončit potřebným krokem $\frac{n^2}{n^2-1} < 1$, protože to neplatí.

Kde je zádrhel? Označme $a_n = \frac{n-1}{n}$. My jakoby víme, že $a_n < 1$, a chceme to použít k důkazu $a_{n+1} < 1$. Když se na ta čísla podíváme blíže, tak zjistíme, že a_{n+1} je mnohem blíže k 1 než výraz a_n. Pokud tedy při úpravách členu a_{n+1} použijeme onen větší rozdíl (což právě při aplikaci indukčního předpokladu děláme), dostaneme se okamžitě nad jedničkua je to v háji.

Závěr je, že vlastnost $V(n)$ indukcí takto přímo dokázat nejde.

Pro další příklad viz cvičení 5a.7.

△

Teď se zase vrátíme ke správným důkazům a ukážeme trochu jiné použití.

! Příklad 5a.i: V tomto příkladě zabrousíme do algoritmizace.

Definujeme rekurzivní proceduru, záměrně se nedržíme nějakého konkrétního jazyka.

```
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 indukcí: $V(n)$ je tvrzení, že výstup *factorial*(n) je $n!$.

(0) $n = 0$: ano, podle specifikace je *factorial*$(0) = 1 = 0!$.

(1) Nechť $n \in \mathbb{N}_0$. Předpokládejme, že $V(n)$ platí, tedy výstup *factorial*(n) je $n!$. Pak výstup *factorial*$(n+1)$ je roven $(n+1)$·*factorial*(n), což je $(n+1) \cdot n! = (n+1)!$.

Důkaz je hotov.

Připomněli jsme si faktoriál, který se indukcí definuje, obvykle takto:

(0) $0! = 1$.

(1) $(n+1)! = n! \cdot (n+1)$ pro $n \geq 0$.

Není to první takový objekt, se kterým jsme se setkali, již v prvních kapitolách se induktivně definovala mocnina zobrazení T^n či složení konečně mnoha zobrazení. Definování objektů pomocí indukce se hlouběji věnujeme v další kapitole, berte tento příklad jako reklamu.

△

! 5a.7 Poznámka:

Využijme tento příklad k malé exkurzi do oblasti algoritmů. Když nějaký algoritmus navrhneme, tak bychom správně měli dokázat, že vždy dělá to, co má. Pokud je to algoritmus rekurentní, pak je k tomu nejvhodnějším nástrojem indukce, ostatně jsme se o vzájemné provázanosti rekurze a indukce již dříve zmínili.

Obvykle se nezačíná tím, co jsme dělali v příkladu výše, tedy zkoumáním výsledku po doběhnutí algoritmu, ale nejprve se musí dokázat, že algoritmus vůbec doběhne. Zkusme si představit, že onen aloritmus výše poštveme na číslo 1.7. Nás algoritmus zjistí, že to není nula, tudíž zavolá sám sebe znovu, tentokráte 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. Neexistuje obecná metoda, jak zjistit, kterými vstupními daty je možné začít, abychom se nakonec do těch základních dostali. Ukážeme dva příklady, veselý a opravdový matematický, přitom velice jednoduchý.

1) Mnoho autorů knih o algoritmizaci či programování neodolá a dá do Rejstříku řádek „Rekurze – viz Rekurze.“ Jde o rekurzivní algoritmus bez ukončovací podmínky. Takovou chybu ovšem udělá jen začátečník, chytřejší autoři tam píšou toto:

„Rekurze – pokud to ještě nechápete, viz Rekurze.“

Zde podmínka pro ukončení je, ale je asi hned jasné, že u některého čtenáře nemusí dojít k její realizaci.

2) Abychom si ukázali pořádný příklad, představíme si nejprve zobrazení $T\colon \mathbb{N} \mapsto \mathbb{N}$ dané předpisem

$$T(n) = \begin{cases} \frac{1}{2}n, & n \text{ sudé;} \\ 3n+1, & n \text{ liché,} \end{cases}$$

viz cvičení 2b.8. Teď se podíváme, co se stane, když jej začneme aplikovat opakovaně (neboli když uvažujeme mocniny T^m tohoto zobrazení). Když třeba začneme s $n = 13$, tak to je liché, proto $T(13) = 3 \cdot 13 + 1 = 40$. 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. A teď koukněte na tohle:

```
procedure T(n: přirozené číslo)
a := T(n);
if a > 1 then T(a);
```

Toto je jednoduchý rekurzivní program, který, pokud jej zavolám jako $T(13)$, skončí po devíti cyklech. Terminační podmínku má, jenže z toho, co jsme si o zobrazení T řekli, vyplývá, že není známo, zda k ní pro všechna vstupní data tento program někdy dojede. To je smutné, současná věda neumí u tohoto algoritmu dokázat, že vždy skončí.

Při zkoumání problému ukončování běhu algoritmu je dobrým nástrojem tzv. *variant*, což je nějaký parametr, který nabývá přirozených čísel a při každém volání rekurze se zmenšuje. Protože neexistuje nekonečná klesající posloupnost přirozených čísel (viz níže), musí algoritmus, u kterého se nám podaří takový variant identifikovat, také někdy skončit. Například u procedury *factorial* může jako variant sloužit n, zatímco u té procedury s T zatím nikdo nějaký variant nevymyslel.

Protože dokázat terminaci algoritmu je často vysoce náročný úkol, zkoumá se u nich takzvaná *parciální korektnost*, což jsou výroky typu „Pokud vůbec algoritmus skončí, tak se stane toto.“ Například ten zajímavý algoritmus s T je parciálně korektní ve smyslu „Jestliže skončí, tak dá jedničku.“ Ale to už opravdu zabíháme do teorie algoritmů, kde je ovšem indukce jedním z oblíbených nástrojů.

△

! Po tolika příkladech už asi není třeba vysvětlovat, že indukce je velice důležitá. Je proto kritické si položit otázku, nakolik je možné jí věřit. Čtenář si jistě všiml, že jsme princip matematické indukce neuvedli jako větu. Důvod je jednoduchý, je to totiž jeden z axiomů matematiky, viz poznámka 4c.15. Většinou se ale do seznamů základních axiomů nezahrnuje, protože je rovnocenný axiomu jinému, který jsme tu už měli (viz Princip 4c.14).

! **Věta 5a.8.**
Princip matematické indukce je ekvivalentní s principem dobrého uspořádání.

Důkaz (drsný, poučný)**:** 1) Předpokládejme, že princip matematické indukce platí. Chceme ukázat, že $(\mathbb{N}, \leq)$ je dobře uspořádaná množina.

Nechť je tedy M nějaká neprázdná podmnožina $\mathbb{N}$. Definujme vlastnost V takto:

$V(n)$: $\{1, 2, \dots, n\} \cap M = \emptyset$.

Kdyby toto platilo pro všechna n, tak by pro všechna n platilo $n \notin M$, tedy $M = \emptyset$, což je ve sporu s předpokladem, že M je neprázdná.

Vlastnost V tedy neplatí pro nějaké $n \in \mathbb{N}$. Uvažujme tato dvě tvrzení:

(0) $V(1)$ platí.

(1) Pro každé $n \in \mathbb{N}$: Jestliže $V(n)$ platí, pak i $V(n+1)$ platí.

Kdyby platilo (0) a (1), tak by dle principu matematické indukce platilo V pro všechna n, my už ale víme, že to nejde. To znamená, že alespoň jedno z těchto dvou tvrzení není pravdivé.

Jestliže není pravda $V(1)$, tak není pravda $\{1\} \cap M = \emptyset$. To znamená, že $1 \in M$. 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 takové, že neplatí implikace $V(n) \implies V(n+1)$. Pro toto speciální n tedy platí, že $V(n)$ je pravda a $V(n+1)$ je nepravda neboli $\{1, 2 \dots, n\} \cap M = \emptyset$ a $\{1, 2 \dots, n, n+1\} \cap M \neq \emptyset$. To mimo jiné říká, že $n + 1 \in M$.

Protože M neobsahuje čísla $1, 2, \ldots, n$, 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.

2) Opačný směr plyne z věty 5a.13, která zobecňuje indukci i na jiné množiny než $\mathbb{N}$.

□

Dobrá otázka: Proč jsme nepoužili obvyklý trik a nedokazovali indukcí $V(n)$: 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 i jiné důkazy této věty. Ten náš je zajímavý tím, že jakoby staví indukci na hlavu.

Teď si ukážeme ještě jednu aplikaci indukce, bude to reklama na novou verzi.

Příklad 5a.j: Uvažujme množinu M měst, vesnic a vůbec osídlení vybranou porůznu po světě. Po světě také existují rozličné železniční sítě, které do některých z osídlení dosáhnou. Pro $n \in \mathbb{N}$ uvažujme tvrzení $V(n)$:

Libovolná množina M s n sídly se dá rozložit na podmnožiny M_i takové, že $M = \bigcup M_i$, mezi osídleními ze dvou různých M_i, M_j nevede železniční spojení, naopak v každé M_i jsou vždy všechna sídla navzájem propojena.

Čtenáře doufejme napadlo, že vlastně mluvíme o rozkladu množiny na třídy ekvivalence, stačí uvažovat relaci na M danou spojením a dokázat, že jde o ekvivalenci. V této kapitole ale zkusíme žádaný rozklad vyrobit přímo, bez pomoci jiné teorie.

Jak bychom takové skupiny M_i vytvářeli? Vezmeme libovolné osídlení $a_1 \in M$ a do množiny M_1 dáme všechna osídlení z M, do kterých se z a_1 dostaneme vlakem. Je pak jasné, že se dostaneme i mezi libovolnými dvěma osídleními z této množiny, přinejhorším to vezmeme s přestupem v a_1. A co ostatní osídlení? K těm jsme se nedostali z a_1 a díky přestupům je jasné, že se k nim nedostaneme ani z ostatních osídlení v M_1, takže tato M_1 je opravdu odříznuta od zbytku M. Logicky bychom dále vzali nějaké a_2 z toho zbytku a tak dále, to volá po indukci.

(0) Jestliže $n = 1$, pak máme množinu $M = \{a\}$ s jedním osídlením, což je zároveň množina M_1, neboť z a do a se dostanu a nikam jinam ne.

(1) Mějme libovolné $n \in \mathbb{N}$ a předpokládejme, že se nám každá n-prvková množina osídlení rozpadne dle předpisu. Uvažujme teď nějakou množinu s $n+1$ osídleními. Vezměme prvek a_1 a vytvořme množinu M_1, přesně jako jsme to dělali výše. Teď uvažujme $M' = M - M_1$. A máme velký problém, protože vůbec nevíme, jestli M' má n prvků. Pokud ne (což se dá mimochodem čekat), tak je nám indukční hypotéza na nic, my jsme totiž předpokládali její platnost jen pro naše n, pro jiná čísla ne.

△

Jaké je z toho poučení? Že občas potřebujeme něco lepšího než obyčejnou indukci.

!

5a.9. 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 následující předpoklady jsou splněny:
(0) $V(n_0)$ platí.
(1) Pro každé $n \in \mathbb{Z}$, $n \geq n_0$ je pravdivá následující implikace: Jestliže platí $V(k)$ pro všechna $k = n_0, n_0 + 1, \ldots, n$, pak platí i $V(n+1)$.
Potom $V(n)$ platí pro všechna $n \in \mathbb{Z}$, $n \geq n_0$.

Tomuto principu se také říká **úplná indukce**. Anglicky se tomu říká **Strong principle of mathematical induction**. Jeho interpretace je následující. (0) říká, že umíme vylézt na první příčku žebříku. (1) říká, že v případě, že umíme vylézt na prvních n příček, tak umíme vylézt i o jednu výše. Princip pak tvrdí, že umíme vylézt na celý žebřík. Ukážeme si, jak nám to pomůže. Nejprve se vrátíme k příkladu výše.

Příklad 5a.k (pokračování 5a.j)**:** Dokážeme vlastnost $V(n)$ o rozkladu množiny osídlení pomocí silného principu indukce.

(0) Jestliže $n = 1$, pak $V(1)$ platí, to už jsme dělali.

(1) Nechť $n \geq 1$ a předpokládejme, že umíme příslušným způsobem rozložit všechny množiny osídlení o velikosti mezi 1 až n včetně. Mějme teď množinu M s $n+1$ osídleními. Zvolíme prvek a_1 a vybereme do množiny M_1 osídlení a_1 a také všechna osídlení, do kterých se z a_1 dostaneme vlakem. Uvažujme $M' = M - M_1$. Pak je počet osídlení v M' menší než v M, čili je to určitě číslo mezi 1 až n včetně. Podle indukčního předpokladu je tedy možné M' rozdělit na navzájem izolované, ale uvnitř propojené podmnožiny $M_2, M_3, \ldots$. Pak je $M_1, M_2, M_3 \ldots$ žádaný rozklad množiny M a důkaz je hotov.

△

Příklad 5a.l: Ukážeme si 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 $V(n)$: 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 platí $V(1)$, $V(2)$, $\ldots$, $V(n)$, tedy že druhý hráč má výherní strategii na hry, kde je na začátku na obou hromádkách stejně zápalek, a to nejvýše n. Chceme ukázat, že pak má i výherní strategii 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 mají obě hromádky po $n + 1 - r$ zápalkách, kde $1 \leq n + 1 - r \leq n$, má podle indukčního předpokladu druhý hráč výherní strategii.

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).

△

Zdá se tedy, že silný princip indukce je opravdu lepší, protože nám pomohl v situacích, kdy slabý selhal. Ve skutečnosti ale silnější není, je jen pohodlnější pro uživatele. Pro názornou ukázku se vrátíme k poslednímu příkladu.

Příklad 5a.m: Uvažujme hru se zápalkami, ale definujme jinou vlastnost.

$W(n)$: Pokud je na začátku v obou hromádkách stejně zápalek, a to mezi 1 a n, pak má druhý hráč výherní strategii.

Dokážeme indukcí platnost pro $n \in \mathbb{N}$:

(0) $n = 1$: Chceme ukázat existenci výherní strategie druhého hráče pro případ, kdy obě hromádky mají jednu zápalku, to už jsme udělali v předchozím řešení.

(1) Nechť $n \in \mathbb{N}$. Dokazujeme platnost implikace $W(n) \implies W(n + 1)$.

Indukční předpoklad je, že druhý hráč má výherní strategie na všechny hry se shodným počtem zápalek na obou hromádkách, a to počtem mezi 1 a n.

Potřebujeme ukázat, že má výherní strategie na všechny hry se shodným počtem zápalek na obou hromádkách, a to počtem mezi 1 a $n + 1$.

Vezměme tedy dvě shodné hromádky. Pokud je počet zápalek mezi 1 až n, pak přímo aplikujeme indukční předpoklad $W(n)$ a máme výherní strategii pro druhého hráče. Pokud je ten počet roven $n+1$, tak v prvním kole poté, co první hráč odebral nějaké zápalky, druhý hráč dorovná hromádky na stejný počet, který je již nejvýše n. Pokud je to nula, druhý hráč vyhrál, takže ví jak na to, pokud ne, použije indukční předpoklad a má výherní strategii.

△

Tento důkaz byl komplikovanější, takže vidíme, že silný princip nám opravdu může ulehčit práci. Myšlenku použitou v příkladě lze použít obecně jako argument, že z pohledu teoretického jsou oba principy indukce rovnocenné.

Věta 5a.10.
Slabý a silný princip matematické indukce jsou ekvivalentní.

Nejprve musíme pořádně říct, co tím vlastně myslíme. Jednoduše řečeno to znamená, že množina věcí, které lze dokázat slabým principem, je úplně stejná jako množina věcí, které jdou dokázat silným principem.

Důkaz (poučný, drsný)**:** 1) Nejprve předpokládejme, že vlastnost V pro čísla $n \geq n_0$ lze dokázat slabým principem, tedy že jsme její platnost dokázali argumentem, že splňuje následující tvrzení:

(s0) $V(n_0)$ platí.

(s1) Pro všechna $n \geq n_0$: Jestliže platí $V(n)$, tak platí i $V(n+1)$.

Musíme ukázat, že ji lze dokázat také silným principem, tedy chceme ukázat, že platí následující vlastnosti:

(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 $V(n+1)$.

Hned vidíme, že (S0) je pro V splněno, protože je to totéž jako (s0).

Je pro V splněno (S1)? Vezměme si nějaké libovolné $n \geq n_0$ a předpokládejme, že platí $V(n_0)$ až $V(n)$. Takže mimo jiné platí i $V(n)$ a o vlastnosti V víme, že splňuje (s1). Podle toho tedy platí $V(n+1)$, čímž je pravdivost (S1) dokázána.

Takže vlastnost V splňuje podmínky (S0) a (S1) a tudíž je její platnost dokázána pro všechna $n \geq n_0$ pomocí silného principu indukce.

2) Teď předpokládejme, že vlastnost V lze pro $n \geq n_0$ dokázat silným principem, tedy že splňuje (S0) a (S1). Musíme ukázat, že ji lze dokázat také slabým principem.

Splňuje (s0)? Ano, protože je to totéž jako (S0).

Splňuje (s1)? Nejspíše ne. Máme ukázat platnost implikace $V(n) \implies V(n+1)$ pomocí znalosti (S1), začneme tedy předpokládat, že $V(n)$ platí, ale to nám nestačí k tomu, abychom dokázali použít (S1), protože nevíme nic o platnosti $V(n_0)$ až $V(n-1)$.

Důkaz tedy takto jednoduše, jak tomu bylo v 1), nepůjde, musíme použít trik. Definujme novou vlastnost $W(n)$ takto: $W(n)$ platí, jestliže platí $V(k)$ pro $k = n_0, \ldots, n$. Dokážeme teď pomocí slabé indukce tuto vlastnost W.

(s0) Nechť $n = n_0$. $W(n_0)$ znamená, že platí $V(n_0)$, což je pravda dle (S0). Takže (s0) platí.

(s1) Nechť $n \geq n_0$ a předpokládejme, že platí $W(n)$. Podle definice této vlastnosti to znamená, že platí $V(n_0)$ až $V(n)$, odtud ale díky platnosti (S1) pro V odvodíme, že platí $V(n+1)$. Platí tedy $V(n_0)$ až $V(n)$ a také $V(n+1)$, tedy platí $W(n+1)$. Dokázali jsme pravdivost implikace $W(n) \implies W(n+1)$, tedy (s1) platí pro W.

Podle slabého principu indukce dostáváme, že W platí pro všechna $n \geq n_0$, proto podle definice W platí i $V(n)$ pro všechna $n \geq n_0$. Takže jsme V dokázali i pomocí slabého principu.

□

! Kdy budeme chtít použít silnou indukci? Rozhodne rekurentní analýza. Pokoušíme se vyřešit daný problém na určité úrovni. Pokud jej dokážeme vždy vyřešit čistě pomocí znalosti předchozí etapy, pak si vystačíme se slabou indukcí. Pokud ale potřebujeme informaci i dále z minulosti, zejména pokud vlastně ani nevíme přesně, jak daleko do minulosti máme zajít, pak musíme použít silnou indukci.

Existují ale situace, které jsou ještě trochu jiné. Tam sice musíme jít dále do minulosti, takže slabý princip indukce nelze přímo aplikovat, ale víme, že pokaždé musíme jít zpět jen o přesně specifikovaný (a stále stejný) počet kroků. Tato situace je velice specifická, protože pak na ni nelze přímo aplikovat ani silný princip indukce. Abychom to ukázali, připomeneme si jeden klasický příklad.

Jak vyložíme podrobněji v příkladě 10b.b, jistý Fibonacci zkoumal králíky a došel k zajímavému závěru, že chce-li předpovědět, kolik párů bude mít příští rok, tak stačí sečíst počet párů z předchozích dvou let. Takže ke znalosti počtu párů v roce 50 potřebujeme znát počty v letech 48 a 49, ze znalosti z let 89 a 90 zase spočteme stav v roce 91 atd. Princip je velice jednoduchý, tak zkusme začít. Řekněme, že je teď rok 1 a víme, že máme jeden pár králíků. Kolik jich budeme mít v příštím roce? Zatímco u slabé a silné indukce stačí znát jednu výchozí hodnotu, tady je to evidentně málo, protože na výpočet potřebujeme znát dvě předchozí hodnoty!

Takže přidejme výchozí informaci, že příští rok (rok 2) budeme mít také jeden pár, a dál už to jde počítat. V roce 3 budou $1+1=2$ páry, v roce 4 bude dle stavu v letech 2 a 3 celkem $1+2=3$ páry, v roce 5 bude $2+3=5$ párů a tak dále.

Vidíme tedy, že pokud ke znalosti další hodnoty potřebujeme vždy znát m hodnot předchozích, tak k rozběhnutí procesu potřebujeme také znát m hodnot počátečních. Máme tedy situaci, která je indukční, ale nehodí se k ani jednomu ze zatím probraných principů. Abychom se s touto situací uměli vyrovnat, představíme si ještě jednu verzi indukce.

!

5a.11. 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 následující předpoklady jsou splněny:
(0) $V(n_0)$, $V(n_0+1)$, $V(n_0+2)$, ... ,$V(n_0+m-1)$ platí.
(1) Pro každé $n \in \mathbb{Z}$, $n \geq n_0+m-1$ je pravdivá následující implikace: Jestliže platí $V(k)$ pro všechna $k = n-m+1, n-m+2, \ldots, n$, pak platí i $V(n+1)$.
Potom $V(n)$ platí pro všechna $n \in \mathbb{Z}$, $n \geq n_0$.

Indexy ve formulaci principu asi na první pohled vypadají trochu divoce, pomůže, když si představíme konkrétní aplikaci. Pro jednoduchost zvolíme $n_0 = 1$, tedy pracujeme na $\mathbb{N}$, a rozmyslíme si situaci, která se odvolává na $m = 3$ předchozí výsledky. K nastartování procesu pak potřebujeme znát situaci pro $n = 1, 2, 3$, což opravdu odpovídá indexům $n_0, n_0+1, \ldots, n_0+m-1$.

Indukční krok by nás měl zavést o krok dál, než známe. Po kroku (0) má poslední známá situace (to, čemu v indukčním kroku říkáme n) index 3, pak očekáváme informaci o $n+1 = 4$, což je první zatím neznámá situace, souhlasí to. Takže indukční kroky nás zajímají pro $n \geq 3$ neboli pro $n \geq n_0+m-1$, to odpovídá zápisu z principu. My ovšem nepotřebujeme znát jen tuto poslední situaci, ale i několik předchozích tak, aby jich celkem bylo m, takže první situace potřebná pro indukční krok kupředu musí mít index $n-m+1$.

Obecná formulace tedy dává smysl. Naštěstí se nemusíme ty rozsahy indexů učit, důležité je znát princip a v konkrétním příkladě pak rozličné hodnoty vyplynou přirozeně z dané situace.

Poznamenejme, že „modifikovaný princip“ je pracovní název, abychom se na něj mohli v tomto textu odvolávat, tento princip nemá univerzálně přijímaný název.

I tento princip je ve skutečnosti ekvivalentní slabému principu. V jednom směru je to zjevné. Pokud výše použijeme hodnotu $m = 1$, tak dostáváme přímo slabý princip indukce, takže ten náš modifikovaný vlastně zahrnuje slabý princip, tudíž toho dokáže přinejmenším stejně.

Důkaz opačným směrem, že věci dosažitelné modifikovaným principem jdou i pomocí slabého, se dělá podobně jako u Věty 5a.10. Definuje se pomocná vlastnost W, kdy $W(n)$ platí právě tehdy, pokud platí $V(n)$, $V(n+1)$ až $V(n+m-1)$. Detaily necháme na čtenáři. Teď si ukážeme příklad, kdy je modifikovaný princip indukce přirozeným nástrojem.

Příklad 5a.n: Dokážeme, že pomocí mincí s hodnotami 3 a 5 dokážeme přímo vyplatit libovolnou korunovou částku větší než 7. (Tím myslíme, že tuto částku rovnou dáme, bez nějakých fíglů s vracením, to pak jde zaplatit jakákoliv částka.)

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).

Takže pro $n \geq 8$ dokážeme $V(n)$: Je možné vyplatit n korun tříkorunami a pětikorunami.

Použijeme modifikovaný princip indukce, který používá zpětného chodu o tři (tedy $m = 3$). Budeme proto potřebovat také tři počáteční hodnoty.

(0) Snadno ověříme, že platí $V(8)$, $V(9)$ a $V(10)$.

Poznámka: Další hodnotu, kterou potřebujeme ověřit, je 11, tedy první indukční krok musí mít $n+1 = 11$ neboli $n = 10$. Tím je dán rozsah pro další část.

(1) Nechť $n \geq 10$, předpokládejme, že platí $V(n-2)$, $V(n-1)$ a $V(n)$. Potřebujeme ukázat, že platí i $V(n+1)$.

Ale to je snadné. Jestliže $n \geq 10$, pak $n-2 \geq 8$, proto podle indukčního předpokladu dokážeme vyplatit $n-2$. Pak ještě přihodíme tříkorunu a vyplatili jsme $n+1$, přesně jak jsme potřebovali.

Z (0) a (1) vyplývá pravdivost $V(n)$ pro všechna celá čísla $n \geq 8$.

Teoreticky víme, že by tento příklad měl jít řešit i slabou indukcí. Zde to jde dokonce i bez nějaké pomocné vlastnosti W jako v obecném důkazu, dokážeme (slabou) indukcí přímo naši V definovanou výše.

(0) Dokážeme vyplatit $8 = 3+5$, tedy $V(8)$ platí.

(1) Mějme libovolné $n \geq 8$ a předpokládejme, že $V(n)$ platí. Chceme ukázat, že platí i $V(n+1)$.

Podle indukčního předpokladu umíme vyplatit n. Jestli je v tom vyplácení také pětikoruna, tak ji nahradíme dvěma tříkorunami a vyplatili jsme $n+1$, hotovo. Pokud by těch n bylo vyplaceno samými tříkačkami, tak díky $n \geq 8$ musí být nejméně tři. Vezmeme tedy tři konkrétní tříkoruny (celkem 9) a nahradíme je dvěma pětikorunami (celkem 10) a máme vyplaceno $n+1$.

Tím jsme vyčerpali všechny možnosti a důkaz (1) je hotov.

Z (0) a (1) vyplývá pravdivost V pro všechna celá čísla $n \geq 8$.

První způsob byl jednodušší, což není překvapující, lépe se hodil k podstatě problému.
△

Tím jsme probrali všechny základní podoby principu indukce a shrneme si praktické použití.

S Algoritmus 5a.12. pro dokazování klasickou indukcí.
1. Ujasněte si, co vlastně chcete dokazovat, napište to jako vlastnost $V(n)$ závisející na celočíselném parametru n, kde se n bere pro všechna $n \geq n_0$ a n_0 je startovací hodnota.
2. Napište si tvrzení $V(n+1)$ a zkuste najít způsob, jak v tomto tvrzení najít/vytvořit situaci z $V(n)$ či dalších předchozích $V(k)$.
3. Podle **2.** se rozhodněte, kterou verzi indukce použijete. Pokud vám k $V(n+1)$ stačí $V(n)$, je slabý princip nejlepší. Pokud potřebujete více předchozích hodnot, ale vždy stejný počet $n-m+1$, $n-m+2$ až n, modifikovaný princip může být tím nejlepším. Pokud se vracíte do minulosti nepravidelně, je to příklad na silný princip indukce.
4. Rozmyslete si, které hodnoty musíte znát na počátku, aby se proces indukce mohl rozběhout. Pak si rozmyslete, která hodnota n vám pro $n+1$ dá první neznámou situaci. Tím je určen rozsah pro indukční krok.
5. Proveďte vlastní důkaz:
a) Dokažte platnost $V(n)$ pro počáteční hodnoty rozmyšlené v bodě **4.**;
b) Zvolte libovolné n z rozsahu rozmyšleného pro indukční krok v bodě **4.**, stanovte indukční předpoklad a s jeho pomocí dokažte platnost $V(n+1)$.
6. Zkontrolujte, že důkaz v části **5 b)** je správný, tedy vychází z toho, co předpokládáte jako pravdivé, a po korektních krocích končí tím, co chcete dokázat.
△
Předchozí příklady tento algoritmus snad dostatečně ilustrovaly, pokud čtenáři ještě nejsou některé úvahy úplně jasné, tak si zkusí spočítat příklady třeba ze cvičení 5a.15, 6a.13, 5b.4 a 5b.5.

Základní blok této kapitoly uzavřeme doplněním směru, který jsme vynechali v důkazu věty 5a.8. Připomeňme, že jsme již dokázali, že ze slabého principu indukce plyne platnost principu dobrého uspořádání. ve Větě 5a.10 jsme pro změnu odvodili, že slabý princip plyne ze silného. Abychom kolečko uzavřeli, potřebujeme ukázat, že silný princip indukce plyne z principu dobrého uspořádání. My ukážeme dokonce něco mnohem obecnějšího.

Věta 5a.13. (o dobře uspořádané indukci)
Nechť $(A, \preceq)$ je dobře uspořádaná množina. Nechť $V(a)$ je vlastnost prvků $a \in A$.
Předpokládejme, že je splněna následující podmínka zvaná **indukční krok**:
Pro všechna $a \in A$ platí: Jestliže $V(x)$ platí pro všechna $x \in A$ splňující $x \prec a$, pak platí i $V(a)$.
Pak platí $V(a)$ pro všechna $a \in A$.

Důkaz (poučný)**:** Nepřímý důkaz neboli dokážeme obměnu implikace „indukční krok $\Longrightarrow$ platnost V“. Předpokládejme, že není pravda, že V platí pro všechna $a \in A$. Ukážeme, že pak neplatí ani indukční krok.

Jestliže není $V(x)$ 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. Označme $X = \{x \in A;\ x \prec a\}$. Indukční krok pro naše a lze teď přepsat takto:

(I) Jestliže $V(x)$ platí pro všechna $x \in X$, pak platí i $V(a)$.

Všimněte si, že a coby nejmenší prvek M splňuje $a \in M$, tedy $V(a)$ neplatí. Abychom tedy ukázali neplatnost této implikace, stačí ukázat, že je splněn její předpoklad. To uděláme rozborem podle toho, jaké je X.

Jestliže je X prázdná, tak je předpoklad implikace automaticky splněn a implikace neplatí.

Druhá možnost je, že X prázdná není. Tyto prvky ovšem nemohou být z M, protože kdyby bylo nějaké $x \in M \cap X$, tak a jako nejmenší prvek M splňuje $a \preceq x$, $x \in X$ zase dává $x \prec a$ a máme spor, viz Lemma 4b.4 (ii).

To znamená, že prvky z X nejsou v M, jinak řečeno, $V(x)$ pro ně platí. Takže zase je předpoklad implikace (I) splněn a implikace tím pádem neplatí.

Více možností pro X (prázdná-neprázdná) není, takže ve všech případech (I) neplatí a důkaz je hotov.
□

Opravdu již tato věta dává hledanou implikaci? Množina $(\mathbb{N}, \leq)$ je dobře uspořádaná, tudíž podle právě dokázané věty k důkazu platnosti nějaké vlastnosti V na $\mathbb{N}$ stačí dokázat následující implikaci:
(I) Nechť $n \in \mathbb{N}$. Jestliže V platí pro všechna $k < n$, pak platí i pro $V(n)$.
Co to znamená? Pokud posuneme index o jedničku (substituce $n' = n-1$, chcete-li, teď $n' \in \mathbb{N}_0$), pak to říká následující: „Jestliže V platí pro všechna $k \leq n$, pak platí i pro $n+1$“, což je přesně krok (1) ze silné indukce.

Počkat, řekne teď pozorný student, a co krok (0)? Ten je v tom schován také, ale trikem. Co když tu původní implikaci (I) aplikujeme na $n = 1$ (popřípadě tu přepsanou na $n = 0$)? Dostáváme výrok „Jestliže V platí pro všechna k splňující $k \in \mathbb{N}$, $k < 1$, tak platí i $V(1)$“. Jsme tedy v situaci, kdy se snažíme dokázat $V(1)$ za pomocí předchozích případů, jenže ony žádné takové nejsou. Nezbývá tedy, než dokázat $V(1)$ přímo, čímž vznikne základní krok (0). Máme tedy celou silnou indukci.

Obecný princip silné indukce, tak jak jsme jej fomulovali, pak dostáváme obdobnou úvahou aplikovanou na množinu $(\{n_0, n_0+1, n_0+2, \dots\}, \leq)$, pro $n_0 \in \mathbb{Z}$. Poučení tedy je, že vlastně existuje jen jeden princip indukce, velmi obecný (tak to vidí lidé zabývající se základy matematiky), ale pro pohodlí praktického uživatele si z něj vytváříme různé podverze, další ještě přibude v následující kapitolce.

Zajímavé je, že indukci můžeme používat i na jiných množinách než $\mathbb{N}$. I pak se v konkrétních případech ověřování indukční implikace rozpadá fakticky na dva případy:

(0) Nechť m je nejmenší prvek m množiny A. Pak je množina $\{x \in A;\ x \prec a\}$ prázdná, což znamená, že předpoklad implikace „Jestliže $V(x)$ platí pro všechna $x \in A$ splňující $x \prec m$, pak platí i $V(m)$“ je vždy splněn automaticky. Proto k důkazu její platnosti musíme ukázat, že $V(a)$ platí vždycky, tedy dokazujeme to bez pomoci ostatních $V(k)$ jinými slovy to je ten základní krok.

(1) Jestliže a není nejmenší prvek množiny A, pak je $\{x \in A;\ x \prec a\}$ neprázdná a my máme při důkazu implikace k dispozici indukční předpoklady, přesně jak jsme zvyklí u indukčního kroku.

Z praktického pohledu tedy děláme věci jako obvykle, nicméně matematici znalecky ocení, že se nám to ve větě podařilo chytře vyjádřit jednou implikací. Je to elegantní, je to přesné, je to záhadné, tak to máme rádi.

Poznámka: Indukci lze dokonce použít i na množinách, na kterých nemáme plnou sílu částečného uspořádání. Například lze dokázat, že princip matematické indukce platí na **ostře uspořádané** množině $(A, \prec)$ právě tehdy, když je tato množina fundovaná (viz 4d).

Poznámka: Jak jsme již viděli, indukci lze používat i u jiných množin než $\mathbb{N}$. V mnoha případech je vcelku zjevné, jak princip indukce modifikovat.

A) Chceme-li dokázat vlastnost V o sudých nezáporných číslech, uděláme to takto:
(0) $V(0)$ platí.
(1) $V(n) \implies V(n+2)$ platí pro $n \geq 0$.
Pokud bychom chtěli jen kladná sudá čísla, začali bychom dvojkou.

B) Chceme-li dokázat vlastnost V o kladných lichých číslech, uděláme to takto:
(0) $V(1)$ platí.
(1) $V(n) \implies V(n+2)$ platí pro $n \geq 0$.

C) Chceme-li dokázat vlastnost V o číslech typu 13^n, uděláme to takto:
(0) $V(1)$ platí.
(1) $V(n) \implies V(13n)$ platí pro $n \geq 1$.
Opravdu? Dle (0) platí $V(1)$. Podle (1) pak platí i $V(13 \cdot 1) = V(13)$. A znovu (1) s předpokladem $V(13)$ dává platnost $V(13 \cdot 13) = V(13^2)$. A znovu (1) s předpokladem $V(13^2)$ dává $V(13 \cdot 13^2) = V(13^3)$ a tak dále.
Pozor, pokud uděláme toto:
(0) $V(0)$ platí,
(1) $V(n) \implies V(13n)$ platí,
tak tím dokážeme jen $V(0)$! Proč? Podle (0) dostanene platnost $V(0)$. Pak aplikujeme (1) a dostaneme platnost pro $V(13 \cdot 0) = V(0)$, oops.
△

Tím už se ale vlastně dostáváme ke strukturální indukci, což je téma příští kapitolky.

5a.14 Poznámka: Pro doplnění ještě uvedeme jeden ekvivalentní indukční princip, který se někdy používá. Česky se mu říká „sestupná indukce“, ale od indukce zatím probrané se liší tím, že sestupnou indukcí platnost vlastnosti vyvracíme.

! **5a.15. Princip sestupné indukce (Infinite descent proof).**
Nechť $V(n)$ je vlastnost přirozených čísel.
Předpokládejme, že je splněn následující předpoklad:
(1) Pro každé $n \in \mathbb{N}$ je pravdivá implikace:
Jestliže platí $V(n)$, pak existuje $k \in \mathbb{N}$ takové, že $k < n$ a $V(k)$ platí.
Potom $V(n)$ neplatí pro žádné $n \in \mathbb{N}$.

Argument, proč toto funguje, je následující: Kdyby náhodou $V(n)$ platilo pro nějaké n, tak by to podle (1) muselo platit i pro menší číslo, takže podle (1) pro ještě menší číslo a tak dále, jenže problém máme v tom, že v $\mathbb{N}$ není pro takovýto nekonečný řetězec zmenšujících se čísel místo, protože je ta množina „dole“ useknutá. Řečeno formálně, princip sestupné indukce je ekvivalentní faktu, že neexistuje nekonečná klesající posloupnost přirozených čísel, čímž jsme u pojmu fundovanosti z kapitoly 4d. není těžké dokázat, že i tento princip je ekvivalentní ostatním principům indukce a principu dobrého uspořádání.

Jako příklad si ukážeme, jak se dá tímto principem zapsat známý Euklidův důkaz, že $\sqrt{2}$ není racionální číslo. Definujme tuto vlastnost:
$V(n)$ říká, že 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 $n \in \mathbb{N}$.
Abychom to dokázali, ukážeme pravdivost (1). 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.
Tím je tedy (1) ověřeno a podle principu sestupné indukce to již dokazuje, že žádné $V(n)$ nemůže platit.

Je samozřejmě možné pomocí tohoto principu také vlastnosti dokazovat jednoduchým trikem, kdy si jako V vezmeme negaci dokazované vlastnosti, pak V vyvrátíme a tím ta původní vlastnost musí platit.
△

A to už bylo opravdu to poslední z této kapitoly.

Cvičení

Cvičení 5a.1 (rutinní, zkouškové)**:** Dokažte, že následující vzorce platí pro všechna $n \in \mathbb{N}$:
(i) $2 + 4 + 6 + \cdots + (2n) = n(n+1)$;
(ii) $1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1)$;
(iii) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$;
(iv) $\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \cdots + \frac{1}{(2n-1)\cdot(2n+1)} = \frac{n}{2n+1}$;
(v) $1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1$;
(vi) $1 + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!} \leq 2 - \frac{1}{n!}$;
(vii) $1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$;
(viii) $n! < n^n$ (toto pro $n \geq 2$).

Cvičení 5a.2 (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 $x_1, \ldots, x_n \in \mathbb{R}$, pak $\left|\sum_{k=1}^{n} x_k\right| \leq \sum_{k=1}^{n} |x_k|$.

Cvičení 5a.3 (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 5a.4 (poučné)**:** Uvažujte vlastnost $V(n)$: $1 + 2 + 3 + \cdots + n = \frac{1}{2}(n-1)(n+2)$.
Ukažte, že $V(n) \implies V(n+1)$ pro všechna $n \in \mathbb{N}$.
Platí $V(n)$?

Cvičení 5a.5 (poučné)**:** Uvažujte vlastnost $V(n)$: $2 + 4 + 6 + \cdots + 2n = n^2 + n - 13$.
Ukažte, že $V(n) \implies V(n+1)$ pro všechna $n \in \mathbb{N}$.
Platí $V(n)$?

Cvičení 5a.6 (poučné)**:** Pokusíme se sečíst všechna čísla typu $\frac{1}{k}$. Definujme

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

Dokažte, že pro všechna $n \in \mathbb{N}$ platí následující:
(i) $H(1) + H(2) + \cdots + H(n) = (n+1)H(n) - n$.
(ii) $H(2^n) \leq 1 + n$.
(iii) $H(2^n) \geq 1 + \frac{n}{2}$.
Nápověda: $\frac{1}{2^n+1} \geq \frac{1}{2^{n+1}}$, $\frac{1}{2^n+2} \geq \frac{1}{2^{n+1}}$, $\ldots$, $\frac{1}{2^n+2^n-1} \geq \frac{1}{2^{n+1}}$, $\frac{1}{2^n+2^n} = \frac{1}{2^{n+1}}$.
Poznámka: Z (iii) hned vidíme, že nekonečný součet $1 + \frac{1}{2} + \frac{1}{3} + \cdots$ nemůže být konečné číslo.

Cvičení 5a.7 (poučné)**:**
(i) 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.
(ii) Uvažujme $W(n)$: $\frac{1}{2}\cdot\frac{3}{4}\cdots\frac{2n-1}{2n}<\frac{1}{\sqrt{3n+1}}$. Dokažte, že platí pro $n\geq 2$.
(iii) Dokažte, že $V(n)$ platí pro všechna $n\in\mathbb{N}$.

Cvičení 5a.8 (rutinní, poučné)**:** Nechť $n\in\mathbb{N}$, $n\geq 2$. Uvažujme množiny $A_1,\ldots,A_n,A_{n+1}$ a zobrazení T_i: $A_i\mapsto A_{i+1}$ pro $i=1,\ldots,n$. Dokažte, že jestliže jsou všechna tato zobrazení invertibilní, pak je invertibilní i $T_n\circ\cdots\circ T_1$ a $(T_n\circ\cdots\circ T_1)^{-1}=T_1^{-1}\circ\cdots\circ T_n^{-1}$ (viz Věta 2b.6 a 2b.7).

Cvičení 5a.9 (rutinní, poučné)**:** Nechť T: $A\mapsto A$ je invertibilní zobrazení. Dokažte, že pro $n\in\mathbb{N}$ platí $(T^n)^{-1}=(T^{-1})^n$ (viz Věta 2b.7).

Cvičení 5a.10 (rutinní, poučné)**:** Nechť $n\in\mathbb{N}$, $n\geq 2$. Uvažujme množiny $A_1,\ldots,A_n,A_{n+1}$ a zobrazení T_i: $A_i\mapsto A_{i+1}$ pro $i=1,\ldots,n$. Dokažte následující:
(i) Jestliže jsou všechna tato zobrazení prostá, pak je prosté i $T_n\circ\cdots\circ T_1$.
(ii) Jestliže jsou všechna tato zobrazení na, pak je na i $T_n\circ\cdots\circ T_1$.
(iii) Jestliže jsou všechna tato zobrazení bijekce, pak je bijekce i $T_n\circ\cdots\circ T_1$.
(Viz Fakt 2b.10.)

Cvičení 5a.11 (zkouškové)**:** Dokažte, že jsou-li A_i pro $i=1,2,\ldots,n$ konečné množiny, pak je i $\bigcup_{i=1}^{n}A_i$ konečná a $\left|\bigcup_{i=1}^{n}A_i\right|\leq\sum_{i=1}^{n}|A_i|$.
Jsou-li navíc navzájem disjunktní, tak $\left|\bigcup_{i=1}^{n}A_i\right|=\sum_{i=1}^{n}|A_i|$.
(Viz Věta 2c.7 a 2c.8.)

Cvičení 5a.12 (poučné)**:** Dokažte tzv. Bernoulliho nerovnost: Jestliže $h>-1$, pak $(1+h)^n\geq 1+hn$ pro všechna $n\in\mathbb{N}_0$.

Cvičení 5a.13: Dokažte indukcí, že $(a-b)$ dělí (a^n-b^n) pro všechna $n\in\mathbb{N}$.

Cvičení 5a.14 (zkouškové)**:** 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 5a.15 (poučné)**:** Hra Nim se hraje takto. Na začátku je hromádka s n zápalkami. Hrají střídavě dva hráči, každý z nich v jednom tahu odebere 1,2 nebo 3 zápalky. Hráč, na kterého zbyde poslední zápalka, prohrává. Dokažte, že jestliže n po dělení 4 dá zbytek 1, tak má druhý hráč výherní strategii. Jinak má výherní strategii první hráč.
Nápověda: Rozmyslete si, že jestliže je na tahu soupeř a je tam přesně 5 zápalek, tak ať už udělá cokoliv, dokážete zahrát tak, aby v dalším tahu prohrál.

Cvičení 5a.16 (poučné)**:** Teď si trochu pohrajeme se šířením neoficiálních informací. Představme si n osob, každá z nich zná na začátku určitou informaci, kterou ostatní neznají. Tyto osoby začnou spolu porůznu po dvou hovořit, a vždy když dvě osoby spolu hovoří, tak si sdělí vše, co zrovna znají.
Označme jako $G(n)$ nejmenší počet takových vzájemných rozhovorů nutný k tomu, aby nakonec všichni věděli všechno.
Je snadné si rozmyslet, že $G(1)=0$, $G(2)=1$, $G(3)=3$, $G(4)=4$.
Dokažte, že $G(n)\leq 2n-4$ pro všechna n.
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:
5a.1: (i): (0) $V(1)$ říká $2=1\cdot 2$, platí. (1) Nechť $n\in\mathbb{N}$. Předpoklad: $2+4+6+\cdots+(2n)=n(n+1)$.
Dokázat: $2+4+6+\cdots+(2n+2)=(n+1)(n+2)$. Dekompozice:
$2+4+6+\cdots+(2n+2)=[2+4+6+\cdots+(2n)]+(2n+2)=[n(n+1)]+(2n+2)=n^2+3n+2=(n+1)(n+2)$.
(ii): (0) $V(1)$ říká $1=\frac{1}{2}1\cdot 2$, platí. (1) Nechť $n\in\mathbb{N}$. Předpoklad: $1+2+3+\cdots+n=\frac{1}{2}n(n+1)$.

Dokázat: $1+2+3+\cdots+(n+1)=\frac{1}{2}(n+1)(n+2)$. Dekompozice:
$1+2+3+\cdots+(n+1)=[1+2+3+\cdots+n]+(n+1)=\left[\frac{1}{2}n(n+1)\right]+(n+1)=\frac{1}{2}(n^2+3n+2)=\frac{1}{2}(n+1)(n+2)$.
(iii): (0) $V(1)$ říká $1^2=\frac{1}{6}1\cdot2\cdot3$, platí. (1) Nechť $n\in\mathbb{N}$. Předpoklad: $1^2+2^2+3^2+\cdots+n^2=\frac{1}{6}n(n+1)(2n+1)$.
Dokázat: $1^2+2^2+3^2+\cdots+(n+1)^2=\frac{1}{6}(n+1)(n+2)(2n+3)$. Dekompozice:
$1^2+2^2+3^2+\cdots+(n+1)^2=[1^2+2^2+3^2+\cdots+n^2]+(n+1)^2=\left[\frac{1}{6}n(n+1)(2n+1)\right]+(n+1)^2=$
$=\frac{1}{6}(2n^3+9n^2+13n+6)=\frac{1}{6}(n+1)(n+2)(2n+3)$.
(iv): (0) $V(1)$ říká $\frac{1}{3}=\frac{1}{3}$, platí. (1) Nechť $n\in\mathbb{N}$. Předpoklad: $\frac{1}{1\cdot3}+\frac{1}{3\cdot5}+\cdots+\frac{1}{(2n-1)\cdot(2n+1)}=\frac{n}{2n+1}$.
Dokázat: $\frac{1}{1\cdot3}+\frac{1}{3\cdot5}+\cdots+\frac{1}{(2n+1)\cdot(2n+3)}=\frac{n+1}{2n+3}$. Dekompozice: $\frac{1}{1\cdot3}+\frac{1}{3\cdot5}+\cdots+\frac{1}{(2n+1)\cdot(2n+3)}=$
$=\left[\frac{1}{1\cdot3}+\frac{1}{3\cdot5}+\cdots+\frac{1}{(2n-1)\cdot(2n+1)}\right]+\frac{1}{(2n+1)\cdot(2n+3)}=\left[\frac{n}{2n+1}\right]+\frac{1}{(2n+1)\cdot(2n+3)}=\frac{2n^2+3n+1}{(2n+1)(2n+3)}=\frac{n+1}{2n+3}$.
(v): (0) $V(1)$ říká $1\cdot1=2-1$, platí. (1) Nechť $n\in\mathbb{N}$. Předpoklad: $1\cdot1!+2\cdot2!+\cdots+n\cdot n!=(n+1)!-1$.
Dokázat: $1\cdot1!+2\cdot2!+\cdots+n\cdot n!+(n+1)\cdot(n+1)!=(n+2)!-1$. Dekompozice:
$1\cdot1!+2\cdot2!+\cdots+n\cdot n!+(n+1)\cdot(n+1)!=[1\cdot1!+2\cdot2!+\cdots+n\cdot n!]+(n+1)\cdot(n+1)!==[(n+1)!-1]+(n+1)\cdot(n+1)!=$
$(n+1)!+(n+1)\cdot(n+1)!-1=(n+2)(n+1)!-1=(n+2)!-1$.
(vi): (0) $V(1)$ říká $1\le2-1$, platí. (1) Nechť $n\in\mathbb{N}$. Předpoklad: $1+\frac{1}{2!}+\frac{1}{3!}+\cdots+\frac{1}{n!}\le2-\frac{1}{n!}$.
Dokázat: $1+\frac{1}{2!}+\frac{1}{3!}+\cdots+\frac{1}{(n+1)!}\le2-\frac{1}{(n+1)!}$. Dekompozice: $1+\frac{1}{2!}+\frac{1}{3!}+\cdots+\frac{1}{(n+1)!}=$
$=\left[1+\frac{1}{2!}+\frac{1}{3!}+\cdots+\frac{1}{n!}\right]+\frac{1}{(n+1)!}\le\left[2-\frac{1}{n!}\right]+\frac{1}{(n+1)!}=2-\frac{(n+1)-1}{(n+1)!}=2-\frac{n}{(n+1)!}\le2-\frac{1}{(n+1)!}$.
(vii): (0) $V(1)$ říká $1\le2-1$, platí. (1) Nechť $n\in\mathbb{N}$. Předpoklad: $1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{n^2}\le2-\frac{1}{n}$.
Dokázat: $1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{(n+1)^2}\le2-\frac{1}{n+1}$. Dekompozice: $1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{(n+1)^2}$
$=\left[1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{n^2}\right]+\frac{1}{(n+1)^2}\le\left[2-\frac{1}{n}\right]+\frac{1}{(n+1)^2}=2-\frac{(n+1)^2-n}{n(n+1)^2}=2-\frac{n^2+n+1}{n(n+1)^2}\le2-\frac{n^2+n}{n(n+1)^2}=2-\frac{1}{n+1}$.
(viii): (0) $V(2)$ říká $2<4$, platí. (1) Nechť $n\ge2$. Předpoklad: $n!<n^n$. Dokázat: $(n+1)!<(n+1)^{n+1}$.
Dekompozice: $(n+1)!=(n+1)n!<(n+1)n^n<(n+1)(n+1)^n=(n+1)^{n+1}$.

5a.2: (0) Pro $n=1$ určitě platí $|x_1|=|x_1|$, platí. (1) Nechť $n\in\mathbb{N}$. Předpokládejme, že platí $\left|\sum_{k=1}^{n}x_k\right|\le\sum_{k=1}^{n}|x_k|$.
Pak $\left|\sum_{k=1}^{n+1}x_k\right|=\left|x_{n+1}+\sum_{k=1}^{n}x_k\right|\le|x_{n+1}|+\left|\sum_{k=1}^{n}x_k\right|\le|x_{n+1}|+\sum_{k=1}^{n}|x_k|=\sum_{k=1}^{n+1}|x_k|$.
5a.3: V indukčním kroku je použito $a^{n-1}=1$, což ale nemusí platit, indukční předpoklad dává jen $a^n=1$.
5a.4: Předpokládejme $1+2+3+\cdots+n=\frac{1}{2}(n-1)(n+2)$. Pak
$1+2+3+\cdots+(n+1)=[1+2+3+\cdots+n]+(n+1)=\frac{1}{2}(n-1)(n+2)+(n+1)=\frac{1}{2}(n^2+3n)=\frac{1}{2}n(n+3)$.
$V(n)$ ale neplatí pro žádné $n\in\mathbb{N}$.
5a.5: Předpokládejme $2+4+6+\cdots+2n=n^2+n-13$. Pak $2+4+6+\cdots+2(n+1)$
$=[2+4+6+\cdots+2n]+(2n+2)=[n^2+n-13]+2n+2=(n^2+2n+1)+(n+1)-13=(n+1)^2+(n+1)-13$.
$V(n)$ ale neplatí pro žádné $n\in\mathbb{N}$.
5a.6: (i): indukcí: (0) $n=1$ dává $1=2\cdot1-1$.
(1) Předpoklad $H(1)+H(2)+\cdots+H(n)=(n+1)H(n)-n$. Pak $H(1)+H(2)+\cdots+H(n+1)=$
$=[H(1)+H(2)+\cdots+H(n)]+H(n+1)=(n+1)\left[1+\frac{1}{2}+\cdots+\frac{1}{n}\right]-n+\left(1+\frac{1}{2}+\cdots+\frac{1}{n+1}\right)=$
$=(n+1)\left(1+\frac{1}{2}+\cdots+\frac{1}{n+1}\right)-(n+1)\frac{1}{n+1}-n+\left(1+\frac{1}{2}+\cdots+\frac{1}{n+1}\right)=(n+2)\left(1+\frac{1}{2}+\cdots+\frac{1}{n+1}\right)-n-1=$
$=(n+2)H(n+1)-(n+1)$.
(ii): Indukcí: (0) $n=1$: $H(2)\le1+1$ znamená $1+\frac{1}{2}\le2$, pravda.
(1) Předpoklad $H(2^n)\le1+n$. Pak $H(2^{n+1})=1+\frac{1}{2}+\cdots+\frac{1}{2^{n+1}}=\left[1+\frac{1}{2}+\cdots+\frac{1}{2^n}\right]+\frac{1}{2^n+1}+\frac{1}{2^n+2}+\cdots+\frac{1}{2^{n+1}}$
$\le1+n+\frac{1}{2^n}+\frac{1}{2^n}+\cdots+\frac{1}{2^n}=1+n+2^n\frac{1}{2^n}=1+(n+1)$, neboť těch zlomků je přesně 2^n, jdou od $\frac{1}{2^n+1}$ po $\frac{1}{2^{n+1}}=\frac{1}{2\cdot2^n}=\frac{1}{2^n+2^n}$.
(iii): Indukcí: (0) $n=1$: $H(2)\ge1+\frac{1}{2}$ znamená $1+\frac{1}{2}\ge1+\frac{1}{2}$, pravda.
(1) Předpoklad $H(2^n)\ge1+\frac{n}{2}$. Pak $H(2^{n+1})=1+\frac{1}{2}+\cdots+\frac{1}{2^{n+1}}=\left[1+\frac{1}{2}+\cdots+\frac{1}{2^n}\right]+\frac{1}{2^n+1}+\frac{1}{2^n+2}+\cdots+\frac{1}{2^{n+1}}$
$\ge1+\frac{n}{2}+\frac{1}{2^{n+1}}+\frac{1}{2^{n+1}}+\cdots+\frac{1}{2^{n+1}}=1+\frac{n}{2}+2^n\cdot\frac{1}{2^{n+1}}=1+\frac{n+1}{2}$.
5a.7: (i): $V(1)$: $\frac{1}{2}<\frac{1}{\sqrt{3}}$ platí.
Zkusíme dokázat indukční krok: Předpoklad $\frac{1}{2}\cdot\frac{3}{4}\cdots\frac{2n-1}{2n}<\frac{1}{\sqrt{3n}}$. Pak
$\frac{1}{2}\cdot\frac{3}{4}\cdots\frac{2n+1}{2n+2}=\frac{1}{2}\cdot\frac{3}{4}\cdots\frac{2n-1}{2n}\cdot\frac{2n+1}{2n+2}<\frac{1}{\sqrt{3n}}\cdot\frac{2n+1}{2n+2}$. Chceme, aby platilo $\frac{1}{\sqrt{3n}}\cdot\frac{2n+1}{2n+2}\le\frac{1}{\sqrt{3(n+1)}}$ neboli
$(2n+1)\sqrt{3(n+1)}\le(2n+2)\sqrt{3n}$, odtud umocněním $n+1\le0$. Toto neplatí nikdy, a protože kroky byly ekvivalentní, nemohla platit ani výchozí nerovnost. Indukční krok se tedy dokázat nepovede.
(ii): (0) $W(2)$: $\frac{1}{2}\,\frac{3}{4}<\frac{1}{\sqrt{7}}$ platí.
Předpokládejme $\frac{1}{2}\cdot\frac{3}{4}\cdots\frac{2n-1}{2n}<\frac{1}{\sqrt{3n+1}}$. Pak $\frac{1}{2}\cdot\frac{3}{4}\cdots\frac{2n+1}{2n+2}=\frac{1}{2}\cdot\frac{3}{4}\cdots\frac{2n-1}{2n}\cdot\frac{2n+1}{2n+2}<\frac{1}{\sqrt{3n+1}}\cdot\frac{2n+1}{2n+2}$. Chceme, aby platilo $\frac{1}{\sqrt{3n+1}}\cdot\frac{2n+1}{2n+2}\le\frac{1}{\sqrt{3(n+1)+1}}$.

Zkusíme postup od konce: přepíšeme nerovnost na $(2n+1)\sqrt{3n+4)} < (2n+2)\sqrt{3n+1}$, odtud umocněním a po úpravě $0 \le n$. To platí, neboť zde máme $n \ge 2$. Všechny kroky byly ekvivalentní včetně umocnění, protože se umocňovala kladná čísla. Postup lze proto obrátit a z pravdivého faktu $0 \le n$ lze korektně dojít k žádané nerovnosti, pomocí ní dokončíme důkaz indukčního kroku:
$\frac{1}{2}\cdot\frac{3}{4}\cdots\frac{2n+1}{2n+2} < \ldots < \frac{1}{\sqrt{3n+1}}\cdot\frac{2n+1}{2n+2} \le \frac{1}{\sqrt{3(n+1)+1}}$.
(iii): $V(1)$ už bylo ověřeno v (i). Pokud $n \ge 2$, pak pomocí $W(n)$ máme $\frac{1}{2}\cdot\frac{3}{4}\cdots\frac{2n-1}{2n} < \frac{1}{\sqrt{3n+1}} < \frac{1}{\sqrt{3n}}$.

5a.8: Indukce: (0) $n=2$: $T_2\circ T_1$ je invertibilní a $(T_2\circ T_1)^{-1} = T_1^{-1}\circ T_2^{-1}$ platí podle Věty 2b.6.
(1) Předpoklad: Pokud $T_1,\ldots,T_n$ splňují předpoklady, pak $T_n\circ\cdots\circ T_1$ je invertibilní a $(T_n\circ\cdots\circ T_1)^{-1} = T_1^{-1}\circ\cdots\circ T_n^{-1}$.
Mějme $T_1,\ldots,T_n,T_{n+1}$ splňující předpoklady, označme $S = T_n\circ\cdots\circ T_1$, podle indukčního předpokladu je S invertibilní a máme vzorec pro S^{-1}. Podle Věty 2b.6 je pak i $T_{n+1}\circ S$ invertibilní a $(T_{n+1}\circ S)^{-1} = S^{-1}\circ T_{n+1}^{-1}$, když dosadíme, dostaneme, že $T_{n+1}\circ T_n\circ\cdots\circ T_1$ je invertibilní a $(T_{n+1}\circ T_n\circ\cdots\circ T_1)^{-1} = T_1^{-1}\circ\cdots\circ T_n^{-1}\circ T_{n+1}^{-1}$.

5a.9: (0) $V(1)$ říká $(T^1)^{-1} = (T^{-1})^1$ neboli $T^{-1} = T^{-1}$, což platí.
(1) Předpokládejme, že $(T^n)^{-1} = (T^{-1})^n$ pro T invertibilní. Mějme teď invertibilní T, označme $S = T^n$. Pak je dle indukčního předpokladu S invertibilní a $S^{-1} = (T^{-1})^n$. Podle Věty 2b.6 je potom $T\circ S$ invertibilní a $(T\circ S)^{-1} = S^{-1}\circ T^{-1}$, po dosazení $(T^{n+1})^{-1} = (T\circ S)^{-1} = S^{-1}\circ T^{-1} = (T^{-1})^n\circ T^{-1} = (T^{-1})^{n+1}$.

5a.10: Hromadný důkaz pro (i) až (iii).
Indukční krok: Předpoklad pro n. Nechť dány $T_1,T_2,\ldots,T_n,T_{n+1}$, které mají příslušnou vlastnost (prosté pro (i), na pro (ii), bijekce pro (iii)). Podle indukčního předpokladu má i $S = T_n\circ\cdots\circ T_1$ příslušnou vlastnost, pak podle Faktu 2b.10 tu vlastnost má i $T_{n+1}\circ S$ neboli $T_{n+1}\circ T_n\circ\cdots\circ T_1$.

5a.11: Indukce, pro $n=1$ evidentně platí.
Indukční předpoklad: tvrzení platí pro n množin. Mějme konečné množiny $A_1,\ldots,A_N,A_{n+1}$. Podle indukčního předpokladu je konečná množina $B = \bigcup_{i=1}^{n} A_i$ a platí $|B| \le \sum_{i=1}^{n}|A_i|$. Pak podle Věty 2c.7 je konečná i množina $B\cup A_{n+1} = \bigcup_{i=1}^{n+1} A_i$ a platí $\left|\bigcup_{i=1}^{n+1} A_i\right| = |B\cup A_{n+1}| \le |B| + |A_{n+1}| \le \sum_{i=1}^{n+1}|A_i|$.
Pokud jso navíc disjunktní, pak podle indukčního předpokladu $|B| = \sum_{i=1}^{n}|A_i|$, množiny B a A_{n+1} jsou disjunktní a proto obdobně $\left|\bigcup_{i=1}^{n+1} A_i\right| = \sum_{i=1}^{n+1}|A_i|$.

5a.12: Indukce: (0) Pro $n=0$ nerovnost říká $(1+h)^0 \ge 1+0$, což platí.
(1) Předpoklad: Dáno $n\in\mathbb{N}_0$, pro každé $h>-1$ platí $(1+h)^n \ge 1+hn$. Pak
$(1+h)^{n+1} = (1+h)(1+h)^n \ge (1+h)(1+hn) = 1+h(n+1)+h^2 \ge 1+h(n+1)$.

5a.13: $a^n - b^b = a^n - a^{n-1}b + a^{n-1}b - b^n = a^{n-1}(a-b) - b(a^{n-1}-b^{n-1})$.

5a.14: (1) Předpokládejme, že $V(n)$ platí. Pak $A^{n+1} = A\cdot A^k = \begin{pmatrix} a & 0\\ 0 & b\end{pmatrix}\cdot\begin{pmatrix} a^k & 0\\ 0 & b^k\end{pmatrix} = \begin{pmatrix} a^{k+1} & 0\\ 0 & b^{k+1}\end{pmatrix}$.

5a.15: $V(n)$: Jestliže je $4n+1$ zápalek, tak má druhý hráč výherní strategii.
(0) $n=0$: Je jedna zápalka, zbyla na prvního hráče, ten prohrál.
(1) Předpoklad: Druhý hráč umí vyhrát hru s $4n+1$ zápalkami. Předpokládejme 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 vyherní 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. Začná hra s $4n+1$ zápalkami, ve které původně první hráč hraje roli druhého a má výherní strategii.

5a.16: 1) Důkaz indukcí: (1) Mějme $n\in\mathbb{N}$, předpokládejme $G(n) \le 2n-4$. Teď uvažujme $n+1$ osob. Jedna z nich někomu ze skupiny řekne svou informaci. Pak se odpojí, zbývající 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 $G(n+1) \le 2n-2 = 2(n+1)-4$. (1) je dokázáno.
2) Důkaz přímý: Pro $1,2,3,4$ to platí. Nechť $n\ge 5$. Označíme si 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?

5b. Rekurze a strukurální indukce

Indukce a rekurze (jak jsme již viděli, jde vlastně o dva pohledy na jednu věc) se často používá i k definování různých objektů. S definicemi indukcí jsme se již setkali v kapitole o množinách, například v definici mocniny T^n pro zobrazení, v předchozí kapitole jsme viděli indukci třeba v definici faktoriálu. Při důkazu korektnosti takové definice hraje obvykle zásadní roli indukce.

Příklad 5b.a: Definujme funkci $f\colon \mathbb{N}_0 \mapsto \mathbb{Z}$ takto:

(0) $f(0) = 1$.

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

Tvrdíme, že f je takto dobře definována pro všechna $n \in \mathbb{N}_0$. Pro ilustraci si to vyzkoušíme. Máme $f(0) = 1$ přímo z definice. Pomocí indukčního kroku použitého s $n = 0$ vidíme, že $f(1) = f(0+1) = -f(0)$ a $f(0)$ již známe, tedy $f(1) = -1$. Teď lze použít (1) s $n = 1$ a dostáváme $f(2) = f(1+1) = -f(1) = 1$, podobně $f(3) = f(2+1) = -f(2) = -1$, $f(4) = f(3+1) = -f(3) = 1$ atd. Zdá se, že opravdu dokážeme najít hodnoty f na $\mathbb{N}_0$, zároveň si můžeme tipnout, že platí $f(n) = (-1)^n$ pro $n \in \mathbb{N}_0$. Jak se dá čekat, takové tvrzení se dá nejlépe dokázat matematickou indukcí.

Pro $n_0 \in \mathbb{N}_0$ dokážeme indukcí vlastnost $V(n)$: Funkce f je dobře definována v n a $f(n) = (-1)^n$.

(0) Pro $n = 0$ to evidentně platí dle (0) v definici.

(1) Nechť $n \in \mathbb{N}_0$. Předpokládejme, že $f(n)$ je definováno a $f(n) = (-1)^n$. Pak podle (1) v definici je definováno i $f(n+1)$ a platí $f(n+1) = -f(n) = -(-1)^n = (-1)^{n+1}$.

Důkaz je hotov.

△

Příklad 5b.b: Definujme funkci $f\colon \mathbb{N} \mapsto \mathbb{Z}$ takto:

(0) $f(1) = 3$, $f(2) = 5$.

(1) $f(n+1) = 2f(n) - f(n-1)$ pro $n \geq 2$.

Spočítáme si nějaké hodnoty. Pokud použijeme (1) s $n = 2$, dostaneme $f(3) = 2f(2) - f(1) = 2 \cdot 5 - 3 = 7$, pak už můžeme použít (1) s $n = 3$ a dostaneme $f(4) = 9$, podobně $f(5) = 11$ a tak dále. Z těchto hodnot odhadneme, že $f(n) = 2n + 1$ pro $n \in \mathbb{N}$ a coby tvrzení $V(n)$ to dokážeme indukcí. Protože k získání $f(n+1)$ potřebujeme znalost dvou předchozích kroků, musíme použít modifikovaný princip s dvěma výchozími hodnotami.

(0) Pro $n = 1$ a $n = 2$ je funkce definovaná a vzorce $f(1) = 2 \cdot 1 + 1$, $f(2) = 2 \cdot 2 + 1$ platí dle (0) v definici.

(1) Nechť $n \in \mathbb{N}$, $n \geq 2$. Předpokládejme, že $f(n)$ a $f(n-1)$ jsou definovány a splňují vzorce z $V(n)$, tedy $f(n) = 2n + 1$ a $f(n-1) = 2(n-1) + 1 = 2n - 1$. Pak je podle (1) v definici dobře definováno i $f(n+1)$ a platí (zase dle (1) z definice a podle indukčního předpokladu), že

$$f(n+1) = 2f(n) - f(n-1) = 2[2n+1] - [2n-1] = 2n + 3 = 2(n+1) + 1,$$

což je přesně vzorec, který jsme potřebovali dokázat.

△

Induktivně lze definovat i množiny. Začneme s přirozenými čísly, které se také musí nějak zavést a Peano je kdysi zadefinoval induktivně takto:

(0) $1 \in \mathbb{N}$.

(1) Jestliže $n \in \mathbb{N}$, pak $n + 1 \in \mathbb{N}$.

Existuje zajímavá souhra mezi induktivní definicí množiny a možností na ni dále budovat nové objekty indukcí, popřípadě na ní indukcí něco dokazovat. Například pokud přijmeme Peanovu definici $\mathbb{N}$ jako platnou (tedy jako axiom), pak z toho dostaneme platnost principu matematické indukce. V klasické teorii množin se ale přirozená čísla dělají jinak, takže princip indukce je třeba přijmout jako samostatný axiom, jak už jsme o tom psali v předchozí kapitole.

Souhru mezi definicí množiny a indukcí si ukážeme na příkladě.

Příklad 5b.c: Množinu A všech kladných sudých čísel lze definovat takto:

(0) $2 \in A$.

(1) $n \in A \implies n + 2 \in A$.

Podrobněji se tímto způsobem definice budeme zabývat za chvíli, zatím nám bude stačit intuitivní představa, že by to mělo fungovat, opakováním kroku (1) do a postupně dodáme všechna kladná sudá čísla.

Když tedy máme induktivně definovanou množinu A, můžeme na ní definovat nový objekt, třeba funkci, přičemž bude třeba zachovávat stejnou indukční strukturu jako v definici A, tedy základní krok musí definovat hodnotu v 2 a indukční krok musí jít ob dva. Vypadá to třeba takto:

(0) $f(2) = 1$.

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

Dostáváme pak například $f(4) = f(2+2) = f(2) + 1 = 2$, $f(6) = f(4+2) = f(4) + 1 = 3$, $f(8) = f(6+2) = f(6) + 1 = 4$ atd.

Tvrdíme, že tato induktivní/rekurzivní definice (vyberte si, které s těch slov se vám víc líbí) definuje f na množině všech kladných sudých čísel a tato funkce splňuje $f(n) = \frac{n}{2}$ pro všechna $n \in A$.

Důkaz provedeme indukcí, kterou ale zase musíme přizpůsobit tomu, jak byla množina A definována.

(0) $n = 0$: funguje to, dle definice $f(2) = \frac{2}{2}$.

(1) Nechť $n \in A$. Předpokládejme, že $f(n)$ je definováno a že $f(n) = \frac{n}{2}$. Pak je podle (1) v definici definováno i $f(n+2)$ a

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

Důkaz je hotov.

Proč by toto mělo stačit? Všechny prvky množiny A (kromě dvojky) se do ní dostaly přičtením dvojky k něčemu, co už v A bylo. Představíme si tedy, jak se množina A postupně rozrůstá. My jsme udělali to, že jsme hned v základním kroku zároveň s přidanou dvojkou pro tu dvojku něco udělali, jmenovitě definovali funkci a pak ukázali určitou vlastnost (funkce je dána pěkným vzoreček). Zároveň jsme nastavili mechanismus, že se při každém přidání dalšího prvku do množiny A na tento nový prvek rozšíří definice funkce, a ještě jsme rovnou dokázali, že když už máme dotyčnou vlastnost (pěkný vzoreček) pro stávající prvky z A, tak se tato vlastnost přenese i na ten nový, který tam právě přidáváme. Je tedy dobré si to představit jako souběžný jev, množinu A zvětšujeme a zároveň si hlídáme, že nové prvky jsou stejně „dobré“ jako ty předchozí. Selský rozum naznačuje, že by pak v A mělo být uvdobré všechno, platnost takovéhoto principu indukce si budeme muset potvrdit řádně matematicky.

Než se do toho dáme, tak poznamenejme, že platnost vzorce $f(n) = \frac{n}{2}$ lze dokázat i jinak. Opět půjde o důkaz blízký tomu, jak množinu A vnímáme. My totiž víme, že lze napsat $A = \{2k;\ k \in \mathbb{N}\}$. Můžeme tedy dokazovat vlastnost $V(k)$: $f(2k) = k$ pro $k \in \mathbb{N}$, což se snadno udělá slabým principem indukce.

△

Teď si přesně zformulujeme induktivní způsob vytváření množin.

5b.1. Induktivní definice množin.
Při definici konkrétní množiny M uvažujme následující dva druhy specifikací:
(0) **Základní pravidla** definují přímo, které prvky jsou v množině M.
(1) **Induktivní 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).

Příklad 5b.d: Vymyslíme pravidla, která definují množinu všech neprázdných (a konečných) binárních řetězců, tedy objektů, které vypadají jako třeba 010010110. Myšlenka je jednoduchá, začne se jedním znakem a k němu budeme přilepovat další, například zprava.

(0) $0 \in M$, $1 \in M$.

(1) Jestliže je r binární řetězec, pak řetězce $r0$ a $r1$ jsou také binární řetězce.

Zdá se zřejmé, že množina M neprázdných binárních řetězců je právě množina dána induktivními pravidly (0) a (1). Například k řetězci „00101“ dojdeme takto:

$$\xrightarrow{(0)} 0 \xrightarrow{(1)} 00 \xrightarrow{(1)} 001 \xrightarrow{(1)} 0010 \xrightarrow{(1)} 00101.$$

Zde je trochu nepříjemné, že ze zápisu vzniku dotyčného řetězce vlastně nevíme, které ze dvou pravidel v (1) jsme použili. Bývá tedy dobré to rovnou v definici udělat pořádně.

(0a) $0 \in M$.

(0b) $1 \in M$.

(1a) $r \in M \implies r0 \in M$.

(1b) $r \in M \implies r1 \in M$.

Pak už máme $\xrightarrow{(0a)} 0 \xrightarrow{(1a)} 00 \xrightarrow{(1b)} 001 \xrightarrow{(1a)} 0010 \xrightarrow{(1b)} 00101$.

Aby byla definice úplná, měli bychom teď správně dokázat, že opravdu množina vytvořená pomocí pravidel (0) a (1) je právě množina všech binárních řetězců. To se obvykle dělá ve dvou krocích, jednak se ukáže, že každý objekt vytvořený pravidly dává neprázdný binární řetězec, a naopak se ukáže, že každý neprázdný binární řetězec lze získat pomocí dotyčných pravidel. Obvykle se využívá klasická indukce, ukážeme si to na nějakém komplikovanějším příkladě.

△

Induktivní definice objektů pomocí pravidel se používá ve více oborech computer science a mnohé z nich si zavádějí své vlastní formální zápisy. My se zde spokojíme se zápisem předvedeným výše, ale pro zajímavost si ukážeme několik jiných formalismů.

1) Při práci s datovými typy se definice zapisují pomocí tzv. *Bakchus-Neurovy formy*, jejíž matematická verze by pro naši množinu vypadala takto:

```
R ::= 0 | 1 | R0 | R1
```

2) Další zajímavý zápis je pomocí *odvozovacích pravidel*. Definice by se u našeho příkladu značily takto:

$$\frac{}{\texttt{0}}(0) \;\Big|\; \frac{}{\texttt{1}}(1) \;\Big|\; \frac{\texttt{s}}{\texttt{s0}}(\_0) \;\Big|\; \frac{\texttt{s}}{\texttt{s1}}(\_1)\ .$$

Odvození řetězce „110“ by se pak napsalo takto:

$$\dfrac{\dfrac{\dfrac{}{1}(1)}{11}(\_1)}{110}(\_0).$$

Pokud se používá tento jazyk, tak se základním pravidlům říká axiomy.

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 stromového schématu. Ukážeme to na nečem, co všichni dobře známe.

Příklad 5b.e: Množinu M korektních algebraických výrazů skládajících se z čísel a malých písmen anglické abecedy lze definovat například takto:

(0a) $a \in M, b \in M, \ldots, z \in M$.

(0b) $\alpha \in \mathbb{R} \implies \alpha \in M$.

(1) Jestliže $\alpha, \beta \in M$, 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 $(1)+\left(\frac{(a)+(b)}{5}\right)$ správně utvořený zápis, ale $\left((1+\frac{a)-5}{3}\right)$ 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 $((2)\cdot(a))+(z)$. Abychom se zbavili zbytečných závorek, museli bychom použít složitější definice. Jedna možnost je již na vstupu zjišťovat strukturu vstupů, třeba pravidly

(1) $a+b, c+d \in M \implies (a+b)\cdot(c+d) \in M$ (zde jsou závorky potřebné)

a

(1) $a+b, c+d \in M \implies a+b+c+d \in M$ (zde závorky nejsou třeba).

Je zřejmé, že pokud bychom chtěli vytvářet výhradně „pěkné“ výrazy, tak by se takových pravidel musela vytvořit spousta, jsou i další problémy. Například nelze přímo zadefinovat pravidlo $a, b \implies a+b$, protože kdyby bylo b záporné, dostali bychom věci jako $23 + -13$. Vytváření pravidel je občas náročné.

Takovéto „gramatiky“ se používají například v teorii jazyků (matematických, programovacích). Ta 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.

△

! **Příklad 5b.f:** Vymyslíme pravidla, která by definovala množinu M všech přirozených čísel, my se ale na ně teď nebudeme dívat jako na čísla, místo toho je budeme vnímat jako obrázky, tedy řetězce určitých značek. Abychom nemuseli psát dvacet pravidel, zavedeme si množinu znaků $C = \{0, 1, 2, 3, \ldots, 8, 9\}$. Čísla pak budeme vytvářet podobně jako v příkladě s binárními řetězci, tedy přilepováním znaků z C, ale bude tu jedna výjimka: Nebudeme ochotni přijmout všechny možné řetězce, nebývá totiž zvykem začínat čísla nulami. Pravidla tedy musíme upravit.

(0) $c \in C - \{0\} \implies c \in M$.

(1) $r \in M \wedge c \in C \implies rc \in M$.

Protože přidáváme další cifry zprava a první cifra je nenulová, vznikají tak zásadně řetězce nezačínající nulou. V tom je jedna z velkých výhod induktivních definic, dají se (někdy) relativně snadno upravit, aby se výsledné množině vnutila nějaká struktura.

Zajímavé je porovnání s oním příkladem 5b.d. Tam bylo v zásadě jedno, jestli se nové znaky přilepovaly zprava nebo zleva, my jsme zvolili zprava čistě proto, že jsme tak zvyklí psát rukou, ale šlo by klidně do (1) dát $0r \in M$ a $1r \in M$. Naopak v tomto příkladě bylo přidávání zprava rozhodující výhodou, protože jsme hned v základním kroku zajistili, že nebudeme mít na levém konci nuly. Pokud bychom se rozhodli přidávat nové znaky zleva, tak bychom museli zajistit, že po každém přidání nul se následně objeví něco nenulového, což se ale induktivními pravidly dle našeho vzoru nedá rozumně zajistit. Jak by to vypadalo?

V kroku (1) by určitě bylo pravidlo $r \in M \ \& \ c \in C - \{0\} \implies cr \in M$. Pak bychom mohli zkusit pravidlo $r \in M \ \& \ c \in C - \{0\} \implies c0r \in M$, jenže tak bychom neuměli vyrobit dvě po sobě jdoucí nuly. Bylo by proto třeba přidat i pravidlo s $c00r \in M$, ale co tři nuly? Protože je možné vyrobit čísla s libovolným počtem po sobě jdoucích nul uprostřed, potřebovali bychom nekonečně mnoho takových indukčních pravidel, což je zjevně slepá ulička.

△

! Příklad 5b.g: Předchozí příklady nás přivádí k zajímavé oblasti zvané teorie jazyků. Ta pracuje obecně s nějakou **abecedou** Σ, což je množina používaných znaků, třeba $\Sigma = \{0, 1\}$ jako v prvním příkladě, C v druhém nebo třeba 26 písmen anglické abecedy. Z těchto znaků pak vytváříme **slova** nad tuto abecedou, což jsou řetězce znaků z abecedy Σ. V teorii jazyků se uvažuje i slovo prázdné, označované λ.

Množina všech slov nad danou abecedou Σ se značí Σ^* a definuje takto:

(0) $\lambda \in \Sigma^*$.

(1) Jestliže $s \in \Sigma^*$ a $x \in \Sigma$, pak $sx \in \Sigma^*$.

V teorii jazyků je základní operací tzv. konkatenace neboli spojování, což už jsme vlastně použili v definici, kdy se dva řetězce spojí za sebe. Například konkatenací slov „auto“ a „drom“ vznikne slovo „autodrom“.

Většinou nepotřebujeme množinu Σ^* všech slov, ale zajímají nás jen slova některá, takže se zavádějí komplikovanější pravidla a gramatiky a teorie jazyků pak začne být velice zajímavá.

Již jsme se zmiňovali, že na množině definované indukcí lze definovat další struktury pomocí indukce stejné formy. Ukážeme si dva zajímavé objekty na množině všech slov.

1) V teorii jazyků se definuje délka slova, a to následovně:

(0) $d(\lambda) = 0$.

(1) Jestliže $s \in \Sigma^*$ a $x \in \Sigma$, pak $d(sx) = d(s) + 1$.

Tím je délka slova definovaná pro všechna slova a snadno si rozmyslíme, že funguje přesně tak, jak bychom čekali. Vlastně jsme tak definovali funkci na Σ^*.

2) Teď zadefinujeme operaci na Σ^*. Operace na množině je procedura, která vezme jeden či více objektů z dané množiny a vrátí nějaký objekt z téže množiny. Nás bude zajímat operace, která dané slovo převrátí, takže bude pozpátku. Pro dané slovo s se výsledek takové operace značí s^R, říkáme tomu *obrácené slovo* a definujeme to takto:

(0) $\lambda^R = \lambda$.

(1) Jestliže $s \in \Sigma^*$ a $x \in \Sigma$, pak $(sx)^R = xs^R$.

Zkusme si obě definice na nějakém příkladě. Vezměme $\Sigma = \{a, b, c, t\}$ a slovo $s = bat \in \Sigma^*$. Jakou má délku?

Neplatí $s \in \Sigma$, proto musíme použít (1) a napsat si s jako spojení $s_1 = ba$ a $x = t$. Podle definice $d(bat) = d(ba)+1$. Voláme rekurzivně (1) a napíšeme si s_1 jako spojení $s_2 = b$ a $x = a$, tedy $d(ba) = d(b) + 1$, nakonec si vyjádříme s_2 coby spojení $s_3 = \lambda$ a b, konečně se dostáváme k něčemu, co umíme. Podle (0) je $d(\lambda) = 0$, zpětným chodem pak $d(b) = 0 + 1 = 1$, $d(ba) = 1 + 1 = 2$ a $d(bat) = 2 + 1 = 3$.

Jak vypadá s^R? Struktura rekurze je obdobná, nejprve podle (1) najdeme $(bat)^R$ jako $t(ba)^R$, pak zase podle (1) je $(ba)^R = ab^R$, nakonec se dostaneme k $b^R = (\lambda b)^R = b\lambda^R = b\lambda = b$. Zpětným chodem pak $(ba)^R = ab$ a $(bat)^R = t(ab) = tab$. Zdá se, že to funguje.

△

Na induktivně definovaných množinách často potřebujeme něco dokázat, například že objekty, které jsme na nich definovaly, splňují nějaké podmínky. Nikterak překvapivě se to dělá indukcí, ale upravenou tak, aby odpovídala definici dotyčné množiny.

5b.2. Princip strukturální indukce (structural induction).
Uvažujme množinu M definovanou induktivně pomocí nějakých základních pravidel (0) a induktivních pravidel (1). Uvažujme vlastnost $V(m)$, která má smysl pro všechna $m \in M$.
Předpokládejme, že jsou splněny následující podmínky:
(0) V je splněna pro všechny prvky, které jsou do M dodány základními pravidly.
(1) Pro každé induktivní pravidlo platí: Jestliže je V splněna pro prvky z jeho předpokladů, pak je splněna i pro prvek z jeho závěru.
Pak je vlastnost V splněna pro všechny prvky $m \in M$.

To je náš poslední indukční princip a ve skutečnosti zase nejde o nic nového, Princip strukturální indukce je ekvivalentní principům z kapitolky 5a. Ještě ale nejsme připraveni to dokázat, necháme si to na konec této kapitoly. Zatím se podíváme na různé příklady a také si představíme nějaké nové myšlenky.

Příklad 5b.h: V tomto příkladě budeme definovat množinu všech řetězců ze symbolů $C = \{1, 2, 3\}$, které neobsahují číslo 11. Hlavní myšlenka je, že postupně přidáváme číslice zprava, ale beztrestně můžeme přidávat jen 2 a 3, protože pak nehrozí nebezpečí vzniku 11. S jedničkou musíme být opatrnější, tu můžeme přidat jen za 2 nebo 3, takže je rovnou přidáme jako dvojice. Tím je jasné, jak bude vypadat (1). Máme ale problém, řetězec „1“ vyhovuje definici, ale nedostaneme jej přidáváním 21 ani 31. Tak tento řetězec zahrneme jako speciální případ do základního pravidla. Dostáváme tedy následující definici množiny M:

(0a) $\lambda \in M$.
(0b) $1 \in M$.
(1a) $w \in M \implies w2 \in M$.
(1b) $w \in M \implies w3 \in M$.
(1c) $w \in M \implies w21 \in M$.
(1d) $w \in M \implies w31 \in M$.

Je tato definice správná? Přesněji řečeno, pokud budeme uvažovat množinu M definovanou induktivně našimi pravidly, bude rovna množině ze zadání? To se obvykle dokazuje dvěma kroky.

1) Dokážeme, že žádný prvek w ze vzniklé množiny M nemůže obsahovat „11“, označíme tuto vlastnost $W(n)$ a podle očekávání použijme strukturální indukci. Při ní musíme sledovat stejnou strukturu jako při definici množiny M, viz Princip strukturální indukce.

(0) Žádný z prvků λ či 1 ze základních pravidel neobsahuje 11, proto je splněno $W(\lambda)$ a $W(1)$.

(1) V tomto kroku potřebujeme ověřit u všech induktivních pravidel, že se platnost W pro prvky z předpokladu přenáší i na prvek ze závěru.

Nejprve uvažujme induktivní pravidlo (1a). Předpokládejme, že řetězec w z jeho předpokladu splňuje $W(w)$, takže neobsahuje 11. Přidáním znaku 2 na konec se to nezmění, tudíž i $W(w2)$ je splněno.

Podobně ukážeme pravdivost implikací $W(w) \implies W(w3)$, $W(w) \implies W(w21)$ a $W(w) \implies W(w31)$ pro zbývající pravidla v (1).

Podle principu strukturální indukce tedy W platí pro všechny prvky množiny M.

2) Teď potřebujeme naopak ukázat, že každý řetězec nad C neobsahující 11 je i v množině M. Uděláme to indukcí na délku řetězce. Dokážeme tedy pro $n \in \mathbb{N}_0$ silnou indukcí tvrzení $V(n)$, že řetězce délky n nad C neobsahující 11 lze vytvořit pomocí (0) a (1). Budeme muset udělat speciální krok pro délku $n = 1$, protože jeden z těchto řetězců, jmenovitě 1, nelze vytvořit z řetězce kratší délky, čímž se vymyká indukci.

(0) Evidentně dokážeme získat řetězce délky 0 a 1, protože řetězec λ je v kroku (0a), řetězec „1“ je v kroku (0b) a ostatní o délce 1, tedy „2“ a „3“ dostaneme kombinací (0a) a (1a) popř. (1b).

(1) Mějme teď $n \in \mathbb{N}$, $n \geq 2$ a předpokládejme, že umíme pomocí pravidel (0) a (1) vyrobit libovolný řetězec délek 0 až n. Uvažujme libovolný řetězec r délky $n + 1$.

Jestliže je jeho poslední znak 3, pak $r = r'3$ pro nějaký řetězec r' délky n, který už podle indukčního předpokladu umíme získat pomocí našich axiomů, z něj pak řetězec r získáme axiomem (1b). Takže r končící na 3 lze vyrobit pomocí pravidel (0) a (1).

Podobně se vyrovnáme s případem, že r končí na 2.

Jestliže r končí na 1, pak předchozí znak (který existuje, $n \geq 2$) musí být buď 2 nebo 3, protože r neobsahuje 11. Předpokládejme první případ, pak $r = r'21$ pro nějaký řetězec r' délky $n - 1$. Odvoláme na indukční předpoklad (tady jsme potřebovali indukci silnou) a pravidlo (1c) a máme r odvozeno, případ $r'31$ se dělá obdobně.

Vyčerpali jsme všechny možnosti, libovolný prvek délky $n + 1$ lze odvodit, tedy $V(n + 1)$ platí. Důkaz je hotov.

Někdy je nám povoleno do pravidel v definici vkládat podmínky. Není to ale tak jednoduché, protože pokud si vezmeme slovo w, tak nemáme nástroj, jak se zeptat na jeho poslední znak. Dá se to elegantně vyřešit tak, že bereme v úvahu jen řetězce jistého typu, například $1w3$ je řetězec, který začíná jedničkou a končí trojkou, pod

jménem w pak máme k dispozici jeho prostřední část. Díky tomu je pak možné vyjádřit induktivní podmínky (1) následovně:

(1a) $w \in M \implies w2 \in M$.
(1b) $w \in M \implies w3 \in M$.
(1c) $w2 \in M \implies w21 \in M$.
(1d) $w3 \in M \implies w31 \in M$.

V některých případech je to výrazně výhodnější, ale ne vždy je nám toto povoleno aplikací, kde induktivní definici používáme.
△

Příklad 5b.i: Mějme abecedu $C = \{0, 1, 2, 3\}$. Zajímá nás množina všech řetězců ze znaků z C, které neobsahují víc nul než jedniček. Abychom ji vybudovali, zkusíme vyjít z klasického postupu, tedy budujeme řetězce postupně, třeba přidáváním zprava. Ze zadání je jasné, že znaky 1, 2 a 3 lze přilepovat bez omezení, ale s přilepováním 0 je třeba být opatrný, musíme zajistit, že za každé přidání se přidá i jednička. Nelze to ovšem udělat přidáním dvojznaku 01, protože odpovídající jednička může být v konečném slově klidně někde jinde, za i před nulou. Nabízí se možnost, že budeme přilepovat 0 na jeden konec a 1 na druhý konec dosavadního řetězce, tedy dvě různá pravidla.

Tím ovšem narážíme na další problém, tímto způsobem nepůjde vyrobit třeba 3120, protože po přilepení 1 zleva a 0 zprava ke dvojce už neumíme přilepovat zleva. Takže se to budeme muset naučit a přidat i přilepování znaků 1, 2, 3 zleva.

Jak bude vypadat základní krok? Začneme řetězci 1, 2 a 3 (řetězec 0 nevyhovuje pravidlům). Docházíme tak k následujícím definicím.

(0a) $1 \in M$.
(0b) $2 \in M$.
(0c) $3 \in M$.
(1a) $r \in M \implies r1 \in M$.
(1b) $r \in M \implies r2 \in M$.
(1c) $r \in M \implies r3 \in M$.
(1d) $r \in M \implies 1r0 \in M$.
(1e) $r \in M \implies 1r \in M$.
(1f) $r \in M \implies 2r \in M$.
(1g) $r \in M \implies 3r \in M$.
(1h) $r \in M \implies 0r1 \in M$.

Je to už dobrá definice? Čtenář teď má příležitost si trochu pohrát a přemýšlet, zda všechny řetězce daného typu, které jej napadnou, dokáže vytvořit pomocí pravidel výše.

Já jsem si docela dlouho myslel, že ano, ale pak mě napadl řetězec 0110, který evidentně pomocí daných pravidel neuklohníme (žádné z nich nemá na krajích nuly).

Jediné rozumné východisko je nějak zařídit, abychom mohli přidávat nulu a jedničku někam doprostřed řetězce. To zní jako dobrý nápad, ale má problém, že když induktivní pravidlo začneme „nechť $w \in M$“, tak to je jeden objekt a my neumíme sáhnout do jeho středu. Budeme tedy rovnou muset začít s jednotlivými úseky, mezi které chceme vsazovat, tedy třemi řetězci. Jenže co když někdy budeme chtít pracovat jen se dvěma segmenty (či jedním)? To hravě vyřešíme zahrnutím prázdného řetězce do naší množiny, čímž si také elegantně zkrátíme základní krok.

(0) $\lambda \in M$.
(1a) $r \in M \implies r1 \in M$.
(1b) $r \in M \implies r2 \in M$.
(1c) $r \in M \implies r3 \in M$.
(1d) $r, s, t \in M \implies r1s0t \in M$.
(1e) $r, s, t \in M \implies r0s1t \in M$.

Máme novou definici a starou otázku: Dá nám všechny řetězce zkoumaného typu? Tentokráte se to opravdu povedlo a ukážeme si alespoň částečně, jak by se to dokazovalo.

1) Vzhledem k tomu, že vždy přidáváme alespoň tolik jedniček co nul, zdá se jasné, že vytvořené řetězce splňují zadání. Formální důkaz se dělá strukturální indukcí a pomůže při něm, když si zavedeme dvě pomocné funkce: $f_0(m)$ udává, kolik je v řetězci m nul, a $f_1(m)$ udává, kolik je v řetězci m jedniček. Uvažujme vlastnost $W(m)$, která říká, že $f_0(m) \leq f_1(m)$. Chceme ukázat, že W platí pro všechny prvky $m \in M$.

(0) Evidentně $f_0(\lambda) = 0 = f_1(\lambda)$, tedy W platí pro všechny prvky ze základních pravidel.

(1) Teď si vezměme nějaké induktivní pravidlo z definice M a předpokládejme, že W platí pro všechny prvky z jeho předpokladu. Rozebereme si případy:

a) Pokud je to pravidlo (1a), tak předpokládáme platnost $W(r)$, tedy že $f_0(r) \leq f_1(r)$. Protože $f_0(r1) = f_0(r)$ a $f_1(r1) = f_1(r) + 1$, dostáváme $f_0(r1) = f_0(r) \leq f_1(r) < f_1(r) + 1 = f_1(r1)$. Takže W platí i pro závěr $r1$ pravidla (1a).

b) Pokud je to pravidlo (1b), tak předpokládáme, že $f_0(r) \leq f_1(r)$. Protože $f_0(r2) = f_0(r)$ a $f_1(r2) = f_1(r)$, dostáváme $f_0(r2) = f_0(r) \leq f_1(r) = f_1(r2)$. Takže W platí i pro závěr pravidla (1b). Podobně se to dokáže případ (1c).

c) Pokud je to pravidlo (1d), tak předpokládáme platnost W pro r, s, t, tedy že $f_0(r) \leq f_1(r)$, $f_0(s) \leq f_1(s)$ a $f_0(t) \leq f_1(t)$. Dostáváme pak $f_0(r1s0t) = f_0(r) + f_0(s) + f_0(t) + 1 \leq f_1(r) + f_1(s) + f_1(t) + 1 = f_1(r1s0t)$. Takže W platí i pro závěr pravidla (1d). Podobně se to dokáže pro (1e).

Podle principu strukturální indukce platí W pro všechna $m \in M$.

2) Teď bychom měli ukázat opačnou inkluzi, tedy že každý řetězec nad C obsahující alespoň tolik jedniček, kolik má nul, leží v naší množině M vytvořené pravidly (0) a (1). Jinými slovy, pro daný objekt musíme vytvořit způsob, kterým jej lze odvodit pomocí pravidel (0) a (1), přičemž ale nevíme, který konkrétní objekt máme, čímž se situace evidentně dosti dramatizuje. Takže tento směr bývá obvykle dosti náročný, zde to proto nedokážeme, spíš zkusíme naznačit, kde je problém.

Obvykle se podobná tvrzení dokazují indukcí, zde bychom použili silnou indukcí na počet nul ve výsledném řetězci. Chtěli bychom dokazovat pro $n \in n_0$ tvrzení $V(n)$, že každý řetězec nad C, který obsahuje n nul a alespoň n jedniček, lze dostat pomocí pravidel (0) a (1).

(0) $n = 0$. Mějme řetězec w, který neobsahuje nuly. Je tedy složen čistě ze znaků 1,2,3. Protože nám pravidla (1) dovolují právě tyto znaky zcela libovolně spojovat za sebe, bude možné vytvořit i řetězec w. To je třeba dokázat a není to příliš obtížné, snadno se to udolá indukcí na délku w.

(1) Mějme $n \in \mathbb{N}_0$. Předpokládejme, že umíme pomocí pravidel sestavit všechny řetězce nad C, které obsahují 0 až n nul a alespoň stejně jedniček. Musíme ukázat, že umíme sestavit i řetězce s $n + 1$ nulami a alespoň $n + 1$ jedničkami. Vezměme si tedy nějaký takový řetězec w.

Základní myšlenka je jasná, chceme využít pravidlo (1) a přejít k podřetězcům, které už budou mít méně nul, pro ně pak využít indukční předpoklad. Takže si v našem řetězci najdeme nějakou nulu a nějakou jedničku, třeba napravo od té nuly. Naše slovo pak lze napsat jako $w = r0s1t$. Pokud bychom byli schopni aplikovat indukční předpoklad na části r, s, t, pak bychom věděli, že je lze pomocí pravidel (0) a (1) vytvořit, další pravidlo (1) už nám dává zkoumané slovo w.

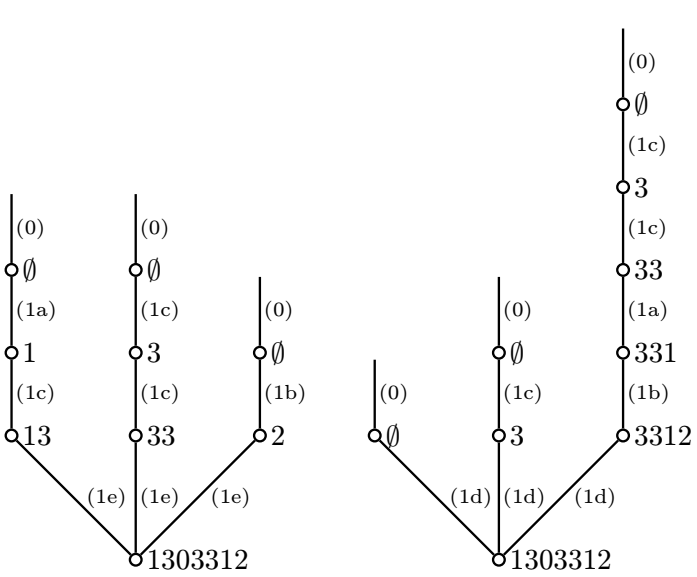
Máme ale velký problém. Protože w mělo $n + 1$ nul a my jsme při vytváření r, s, t jednu nulu z w odebrali, je jasné, že všechny tyto tři části obsahují nejvýše n nul. Není ale žádný důvod, proč by každá z těchto částí měla mít alespoň tolik jedniček, kolik má nul. Jedničky totiž mohly být ve w rozloženy v zásadě libovolně, takže se klidně mohlo stát, že po rozdělení w na části se všechny dostali do jedné z nich, zatímco jiná část má nuly, ale jedničky už na ni nezbyly, na takovou část pak ale nelze aplikovat indukční předpoklad.

Klíčem k úspěchu je tedy vyřešit tento problém dělení w na části. Je třeba ukázat, že lze w rozdělit tak, aby žádná výsledná část neměla méně jedniček než nul. To je kombinatorický problém, který není triviální, takže jím nebudeme tuto kapitolu natahovat.

△

! Když máme množinu M definovanou indukcí, tak se každý prvek z M vytvořil nějakým konečným počtem použití pravidel z (0) a (1), říká se tomu derivační postup a lze jej pěkně znázornit **derivačním stromem** či **odvozovacím stromem** (anglicky **parsing tree**). Prvek je kořenem dole, podle indukčních pravidel (značí se zkratkou vedle hran) se postupně dojde k listům, tj. prvkům ze základních pravidel (0). Počet úrovní stromu (přesněji řečeno největší počet kroků, který je ve stromu možné jedním směrem udělat) je **výška** stromu, takže prvky ze základních pravidel mají výšku 1 (nejprve je nic, jedním krokem dle pravidla (0) se pak dojde k dotyčnému prvku). Má to ale malý zádrhel, může se totiž snadno stát, že se ke zkoumanému prvku dokážeme dostat pomocí pravidel z (0) a (1) více způsoby.

Pro příklad se vrátíme k předchozí definici řetězců s alespoň tolika jedničkami co nulami, najdeme si dva odvozovací stromy pro řetězec 1303312:



Stát se to tedy snadno může. Protože jsou ale výšky všech stromů alespoň jedna, dá se hledat nejnižší možný z nich. Definujeme **výšku prvku** jako nejmenší možnou výšku odvozovacího stromu pro dotyčný prvek. Tím se ale zase poněkud zkomplikuje praktické určování výšky prvku. Nahoře máme dva odvozovací stromy pro 1303312, menší z nich má výšku 4, ale to ještě neznamená, že prvek 1303312 má výšku 4. Museli bychom dokázat, že neexistuje žádný nižší strom pro 1303312 (což je mimochodem pravda).

Poslední příklad ukázal, že strukturální definování množin nemusí být zase tak snadné. Někdy dokonce stačí jen malá modifikace zadání a máme problém, pro ukázku se vrátíme k námětu příkladu 5b.h.

! Příklad 5b.j: V tomto příkladě se pokusíme definovat množinu všech řetězců ze symbolů $C = \{1, 2, 3\}$, které neobsahují číslo 13. To vypadá obdobně jako příklad 5b.h, proto použijeme stejnou myšlenku a budeme postupně přidávát číslice zezadu (zprava) s tím, že beztrestně můžeme přidávat jen 1 a 2, protože pak nehrozí nebezpečí vzniku 13. S trojkou musíme být opatrnější, tu můžeme přidat jen za 2 nebo 3. Pro začátek si ukážeme, jak může vypadat definice, pokud je nám povoleno použít podmínky.

(0a) $\lambda \in M$.
(0b) $3 \in M$.
(1a) $w \in M \implies w1 \in M$.
(1b) $w \in M \implies w2 \in M$.
(1c) $w2 \in M \implies w23 \in M$.
(1d) $w3 \in M \implies w33 \in M$.

Dá se dokázat, že tato definice dělá to, co po ní chceme.

Ne vždy je ovšem toto možné, takže mnohem zajímavější je vytvářet definice bez podmínek. Problémem je přidávání trojky. V příkladě 5b.h jsme toto řešili tak, že jsme přidávali dvojznaky, což by naznačovalo následující definici.

(0a) $\lambda \in M$.
(0b) $3 \in M$.
(1a) $w \in M \implies w1 \in M$.
(1b) $w \in M \implies w2 \in M$.
(1c) $w \in M \implies w23 \in M$.

Proč jsme nezahrnuli pravidlo $w \in M \implies w33 \in M$? Protože pokud by řetězec W končil jedničkou (což může), tak by vzniklo 133 a máme třináctku. Tím ovšem vznikl zásadní problém, protože řetězec 233 je dozajista korektní, ale našimi pravidly jej vytvořit nejde. Proč tedy nepřidat pravidlo?

(1d) $w \in M \implies w233 \in M$.

To je sice pěkné, ale zase neumíme vytvořit 2333. Přidáním

(1e) $w \in M \implies w2332 \in M$

zase nevyřešíme problém řetězce 23333 atd., potřebovali bychom nekonečně mnoho pravidel.

Tudy tedy cestička nevede. Pomohlo by, pokud bychom povolili přidávání i zleva?

(0a) $\lambda \in M$.
(0b) $3 \in M$.
(1a) $w \in M \implies w1 \in M$.
(1b) $w \in M \implies w2 \in M$.
(1c) $w \in M \implies w23 \in M$.

(1d) $w \in M \implies 2w \in M$.
(1e) $w \in M \implies 3w \in M$.
(1f) $w \in M \implies 12w \in M$.

Teď už libovolný řetězec typu 23333 vytvoříme, nejprve opakováním (1e) dodáme ty trojky a pak zakončíme pomocí (1f). Ale pořád neumíme řetězec 11233.

Přiznám se, že se mi nepodařilo vymyslet rozumně krátký soubor axiomů bez podmínek pro řetězce bez 13. Takže strukturální definice je nástroj mocný, ale občas překvapivě obtížný na použití.
△

Příklad 5b.k: Dokonce ani u některých „pěkných“ množin není jasné, jak je efektivně definovat indukcí. Typickým příkladem jsou celá čísla. Když se necháme inspirovat Peanovým pohledem na čísla přirozená, dostaneme toto:

(0) $0 \in \mathbb{Z}$.
(1a) $n \in \mathbb{Z} \implies n+1 \in \mathbb{Z}$.
(1b) $n \in \mathbb{Z} \implies n-1 \in \mathbb{Z}$.

To samozřejmě funguje, ale má to jednu nevýhodu, každé číslo je definované mnohokrát, dokonce nekonečně mnohokrát. Například abychom odvodili číslo 13 z nuly, tak nejprve zopakujeme pravidlo (1a) třeba milionkrát a pak dáme pravidlo (1b) milion mínus 13 krát. Je to tedy velice plýtvavá definice. Mimochodem, jde docela zajímavě smrsknout:

(0a) $0 \in \mathbb{Z}$.
(0b) $1 \in \mathbb{Z}$.
(1) $m, n \in \mathbb{Z} \implies m-n \in \mathbb{Z}$.

Pořád ale strašlivě plýtváme. Jde to lépe? Ano, pokud si dovolíme logiku.

(0) $0 \in \mathbb{Z}$.
(1a) $n \in \mathbb{Z} \wedge n \geq 0 \implies n+1 \in \mathbb{Z}$.
(1a) $n \in \mathbb{Z} \wedge n > 0 \implies -n \in \mathbb{Z}$.

Teď už vůbec neplýtváme, ale takovéto podmínky se zase obtížně vyjadřují některými z používaných formalismů, takže bychom se jim měli spíš vyhýbat. Někdy to prostě ideálně nejde.
△

Ukážeme si ještě dva příklady, kde budeme mít několik příležitostí si indukci vyzkoušet.

Příklad 5b.l (delší pro pokročilé, ale poučný)**:** Dokážeme, že každé symetrické číslo se sudým počtem číslic je dělitelné 11.

Možných přístupů je více, tady to zkusíme přes strukturální indukci. Nejprve taková čísla nadefinujeme. Aby se nám to lépe dělalo, označme si $C = \{1,2,3,4,5,6,7,8,9\}$. Zajímají nás čísla jako 340043, 10377301 či 1331. Taková čísla budeme jistě vytvářet souběžným přidáváním zleva i zprava.

Aby se nám pravidla lépe pilovala, budeme se zatím dívat na čísla jako na řetězce cifer. Po troše přemýšlení čtenáře jistě napadlo, že přidávání je třeba dělat opatrně, problémem je nula. Když třeba k 33 přidáme nulu na obě strany, dostaneme 330, což už není symetrické číslo. Čísla s nulami ale jsou, problém vyřešíme tak, že když přidáváme nulu, tak povinně přidáme i něco jiného.

Čím začneme? Nemůžeme začít prázdným řetězcem (není to číslo), takže v základním kroku budeme muset nastrkat do M všechny možné dvojičky cifer z c. To ale nestačí, jak uděláme číslo 2002? Nelze dát jako základní číslo 00 a pak případně přidat 2 na oba konce, protože to 00 je vlastně 0. Musíme tedy v základním kroku dodat i čísla typu 2002.

(0a) $c \in C \implies cc \in M$.
(0b) $c \in C \implies c00c \in M$.
(1a) $r \in M \wedge c \in C \implies crc \in M$.
(1b) $r \in M \wedge c \in C \implies c0r0c \in M$.

Tato definice je správná a zároveň efektivní, když dostaneme symetrické číslo se sudým počtem číslic, tak jej lze coby řetězec vyrobit jediným způsobem pomocí našich pravidel.

Abychom s tím teď mohli pracovat matematicky (chce se po nás dělitelnost), musíme ty operace s řetězci (spojování neboli konkatenace) přepsat do řeči čísel, což znamená, že si budeme hrát se zápisem čísla v desítkové soustavě. Například chceme-li k číslu r „přilepit“ na konec „38“, tak si nejprve musíme na konci udělat na ty znaky místo a „$r00$“ dostaneme v řeči čísel jako $100 \cdot r$. Znaky pak dolepíme přičtením: $100 \cdot r + 3 \cdot 10 + 8$. Podobné triky teď použijeme k přepisu pravidel výše, čímž dostaneme opravdu množinu čísel, ne řetězců. Označíme ji proto jinak, třeba S, a prvky z C a 0 teď bereme jako čísla.

(0a) $c \in C \implies 10c + c \in S$.

(0b) $c \in C \implies 1000c + c \in S$.

(1a) Jestliže $s = \sum_{i=0}^{m} s_i 10^i \in S$, kde $s_m \neq 0$, a $c \in C$, pak $c \cdot 10^{m+2} + \sum_{i=0}^{m} s_i 10^{i+1} + c = 10^{m+2}c + 10s + c \in S$.

(1b) Jestliže $s = \sum_{i=0}^{m} s_i 10^i \in S$, kde $s_m \neq 0$, a $c \in C$, pak $10^{m+4}c + 100s + c \in S$.

Nejprve si dokážeme že opravdu výsledná čísla mají sudý počet cifer. Použijeme strukturální indukci.

(0) To je jasné, pro $c \in C$ jsou $10c + c$ dvouciferná a $1000c + c$ čtyřciferná.

(1a) Má-li s sudý počet cifer, pak $s = \sum_{i=0}^{m} s_i 10^i$, $s_m \neq 0$ a m je liché (rozmyslete si to). Pak je ale i $m+2$ liché a proto má $10^{m+2}c + 10s + c$ sudý počet cifer.

Důkaz pro (1b) je obdobný.

Víme tedy, že když si vezmeme nějaké $s = \sum_{i=0}^{m} s_i 10^i \in S$, kde $s_m \neq 0$, tak je m liché.

Teď už strukturální indukcí dokážeme to hlavní: Pro každé $s \in S$ platí, že je dělitelné 11.

(0) Nejprve to dokážeme pro prvky ze základních kroků.

(0a) Nechť $c \in C$. Pak $10c + c = 11c$, tedy číslo dělitelné 11.

(0b) Nechť $c \in C$. Pak $1000c + c = 1001c = 11 \cdot 91c$, tedy číslo dělitelné 11.

(1) Teď probereme induktivní pravidla.

(1a) Nechť $s \in S$ a předpokládejme, že je dělitelné 11, tedy $s = 11k$. Víme, že když si zapíšeme $s = \sum_{i=0}^{m} s_i 10^i \in S$, kde $s_m \neq 0$, tak je m liché, $m = 2n-1$. Pak pro $c \in C$ je $10^{m+2}c+10s+c = 10\cdot(11k)+(10^{2n+1}+1)c$. V příkladě 5a.b jsme dokázali, že čísla typu $10^{2n+1} + 1$ jsou také dělitelná 11, tedy $10^{m+2}c + 10s + c = 11 \cdot (10k) + 11l \cdot c = 11a$, i nové číslo je dělitelné 11.

(1b) Nechť $s \in S$ a předpokládejme, že $s = 11k$ pro $k \in \mathbb{Z}$. Podobně jako v (1a) zapíšeme $s = \sum_{i=0}^{m} s_i 10^i \in S$, kde $m = 2n - 1$, a pro $c \in C$ máme $10^{m+4}c + 100s + c = 11 \cdot (10k) + (10^{2(n+1)+1} + 1)c = 11b$, zase je i nové číslo dělitelné 11.

Důkaz je hotov.

tento důkaz nebyl nejefektivnější, ale pěkně ukázal různé aspekty práce s řetězci i čísly a strukturální indukci v akci.

△

Příklad 5b.m: Uvažujme šachovnici „nekonečnou směrem nahoru a doprava“, jejíž políčka jsme si zakódovali pomocí dvojic (i, j) pro $i, j \in \mathbb{N}$, kde i ukazuje vodorovně doprava (tedy udává číslo sloupce) a j ukazuje nahoru. Na levé dolní rohové políčko, tedy na souřadnici $(1, 1)$, položíme šachového koně. To je figurka s nejzajímavějším pohybem, jsou jí totiž povoleny jen tahy ve tvaru L. Přesně řečeno, tah koně se skládá z poskoku o dvě pole v nějakém vodorovném či svislém směru, následovaného poskokem o jedno pole do pravého úhlu.

Tvrdíme, že se kůň pomocí těchto tahů dostane na zcela libovolné pole na naší šachovnici.

Evidentně je to úloha, kterou bychom rádi řešili matematickou indukcí. Problémem ale je, že šachovnice je dvourozměrná. S tím se dá vyrovnat několika způsoby, ukážeme si čtyři.

1) Jedna možnost je si situaci zjednodušit tím, že si pohyb v rámci šachovnice rozložíme do dvou směrů, takže když chceme někam dojít, tak nejdřív jdeme pořád napravo, dokud nebudeme ve správném sloupci, a pak půjdeme nahoru na cílové pole. Pohyb napravo už má jen jeden parametr, stejně tak jako pohyb nahoru, takže tam by měla indukce pomoci.

Zkusíme nejprve indukci slabou, která se odvolává jen na předchozí situaci. Abychom uspěli, musíme vymyslet, jestli se dá někam dostat za předpokladu, že už jsme o políčko vedle (to je ten rekurzivní způsob myšlení). Umíte se nějak koněm dostat o jedno pole doprava, popřípadě nahoru? Rozmyslete si to, já už to umím, a tak vím, že indukce projde.

1a) Nejprve dokážeme, že se z počátku $(1, 1)$ dokážeme dostat libovolně daleko doprava. Formálně:

Pro $i \in \mathbb{N}$ dokazujeme $V(i)$: kůň se umí dostat z pole $(1, 1)$ na pole $(i, 1)$.

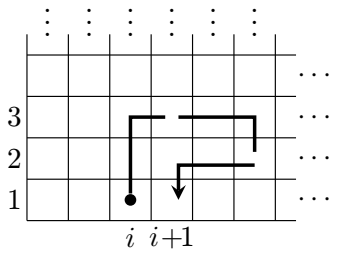
Uděláme to matematickou indukcí.

(0) $i = 1$: Na poli $(1, 1)$ už kůň je, takže se tam určitě umí dostat.

(1) Nechť $i \in \mathbb{N}$ a předpokládejme, že se kůň umí dostat z $(1, 1)$ na pole $(i, 1)$. Chceme ukázat, že se dostane i na pole $(i + 1, 1)$. To se provede následujícími třemi tahy:

tah 1: $(i, 1) \mapsto (i + 1, 3)$,
tah 2: $(i + 1, 3) \mapsto (i + 3, 2)$,
tah 3: $(i + 3, 2) \mapsto (i + 1, 1)$. Takže $V(1)$ platí.

Důkaz $V(i)$ je hotov.



1b) Teď bychom se potřebovali zase posunout nahoru a čtenář by měl mít pocit, že je to vlastně stejný problém, čili důkaz by měl být stejný. Je tomu tak, až na jednu maličkost, teď už totiž nestačí dokazovat cestu vzhůru jen pro první sloupec, ale důkaz musí cestování nahoru potvrdit pro sloupec libovolný, z místa $(m, 1)$, kam jsme došli v první fázi.

Nechť $m \in \mathbb{N}$ je pevně zvolené číslo (parametr). Pro $j \in \mathbb{N}$ dokazujeme $W_m(j)$: kůň se umí dostat z pole $(m, 1)$ na pole (m, j).

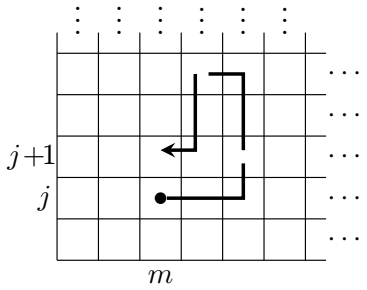
Uděláme to matematickou indukcí.

(0) $j = 1$: Na poli $(m, 1)$ už kůň je, takže se tam umí dostat.

(1) Nechť $j \in \mathbb{N}$ a předpokládejme, že se kůň umí dostat z $(m, 1)$ na pole (m, j). Chceme ukázat, že se dostane i na pole $(m, j + 1)$. To se provede následujícími třemi tahy:

tah 1: $(m, j) \mapsto (m + 2, j + 1)$,
tah 2: $(m + 2, j + 1) \mapsto (m + 1, j + 3)$,
tah 3: $(m + 1, j + 3) \mapsto (m, j + 1)$. Takže $V(1)$ platí.

Důkaz $W_m(j)$ je hotov.

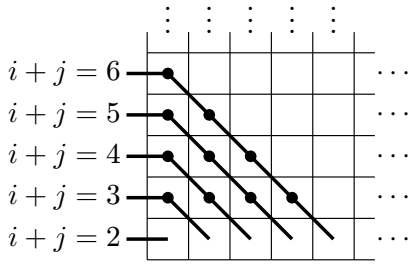


Teď to dáme dohromady. Má-li se kůň dostat na pole (m, n), pak se pomocí vlastnosti $V(m)$ nejprve dostane na pole $(m, 1)$ a pak pomocí vlastosti $W_m(n)$ na pole (m, n). Hotovo.

Všimněte si jedné podstatné věci. Aby byl důkaz úplný, tak je třeba dávat pozor na to, že na ony tři tahy máme vždy na šachovnici místo. To je pravda, protože k přesunu využíváme směry doprava a nahoru, kde je šachovnice neomezená. Ještě se k tomu vrátíme v poznámce na konci příkladu.

2) Někdy je možné se na vícerozměrnou situaci podívat z jiného úhlu pohledu tak, že už se dá popsat jedním parametrem. V tomto případě k tomu dojde, pokud se díváme na pohyb po šachovnici vzhledem k diagonálám. Každá diagonála má své číslo. Dokážeme se dostat na libovolnou danou diagonálu, pokud předpokládáme, že už jsme na diagonále, která je o jedno blíž k počátku? Ano, stačí se posunout o jedno pole doprava či nahoru a to už jsme zvládli. Udělejme to pořádně.

To, na jaké diagonále stojíme, když jsme na poli (i, j), se pozná podle hodnoty součtu $i + j$ (viz obrázek). Tento parametr $n = i + j$ použijeme v naší indukci. Nejmenší možná hodnota je $1 + 1 = 2$. Budeme tedy pro $n \geq 2$ dokazovat tvrzení $V(n)$: Dokážeme se koněm dostat z pole $(1, 1)$ na libovolné pole (i, j) splňující $i + j = n$.



(0) Nechť $n = 2$. Jsme v bodě $(1, 1)$, máme se dostat na bod (i, j) splňující $i + j = 2$, takový bod je jediný, $(1, 1)$, a tam už jsme.

(1) Nechť $n \geq 2$. Předpokládáme platnost $V(n)$, tedy že se umíme dostat z bodu $(1, 1)$ do libovolného bodu (u, v) splňujícího $u + v = n$. Potřebujeme dokázat $V(n + 1)$, tedy že se z bodu $(1, 1)$ dostaneme i do libovolného bodu (i, j) splňujícího $i + j = n + 1$.

Vezměmež si tedy nějaký takový bod (i, j). Jestliže $i > 1$, tak nejsme na levém kraji a můžeme se podívat na bod $(i - 1, j)$ o jedno doleva. Ten splňuje $(i - 1) + j = (i + j) - 1 = n + 1 - 1 = n$ (je na předchozí diagonále), tudíž se tam podle indukčního předpokladu umíme dostat. Zbývá posun o jedno políčko doprava, což už třemi tahy dokážeme, viz předchozí důkaz. Tento případ je tedy hotov.

Jestliže $j > 1$, tak nejsme na dolním okraji a můžeme se podívat na bod $(i, j - 1)$ o jedno níže. Ten splňuje $i + (j - 1) = (i + j) - 1 = n + 1 - 1 = n$, tudíž se tam podle indukčního předpokladu umíme dostat. Zbývá tedy posun o jedno políčko nahoru, což už také třemi tahy dokážeme, viz předchozí důkaz. Tento případ je tedy také hotov. Všimněte si, že pokud náhodou nejsme na nějakém kraji, tak jsou splněny obě podmínky, tudíž máme na výběr, který způsob si vybereme. To není nikterak na závadu, hlavní je, aby alespoň jeden způsob fungoval.

Vyčerpali jsme tím všechny možnosti? Máme $n \geq 2$, takže vlastně uvažujeme body (i, j) splňující $i+j = n+1 \geq 3$, takže alespoň jedno z i, j musí být větší než 1. Jinými slovy, těmito dvěma možnostmi jsme pokryli možnosti všechny a důkaz je hotov.

3) Předchozí důkaz lze v jednom bodě zjednodušit. Všimneme si, že pokud jde kůň tahem od dvě pole dolů a doprava, tak se ocitnul na diagonále s o jedno menším číslem. K přechodu mezi diagonálami v předchozím důkazu tudíž vůbec nemusíme používat trojskok, ale stačí jeden základní tah koněm. Má to ale drobný zádrhel, ne vždy na něj musí být dost místa. Může se stát, že se nedokážeme vrátit o diagonálu zpět? Ano, pokud nemáme ani dvě řady směrem dolů, ani dvě řady směrem doleva. Jinými slovy, problémová jsou pole o souřadnicích $(2, 1)$, $(2, 2)$ a $(1, 2)$. Pokud bychom tedy chtěli důkaz 2) upravit na základní tah koně, musel by vypadat takto:

(0) V základním kroku bychom ukázali, že se lze z $(1, 1)$ dostat na pole (i, j) se součtem $i + j$ rovným 2, 3 a 4, to se prostě jen najdou konkrétní tahy pro tato pole.

(1) V indukčním kroku bychom uvažovali $n \geq 4$. Máme koně na výchozím poli (i, j) splňujícím $i + j = n + 1$, tedy $i + j$ je nejméně 5. Proto určitě $i \geq 3$ nebo $j \geq 3$. V prvním případě uvažujeme pole $(i - 2, j + 1)$. To je na diagonále číslo $(i - 2) + (j + 1) = n$, proto se na něj dle indukčního předpokladu dostaneme, jeden tah koně nás pak doveze na (i, j). V druhém případě použijeme pole $(i + 1, j - 2)$.

4) Další zajímavou možností je použít strukturální indukci. Nejprve si musíme zadefinovat množinu $M = \mathbb{N} \times \mathbb{N}$ pomocí indukčních pravidel, pak se indukcí se stejnou strukturou dokáže vlastnost $V(i, j)$: lze dojet koněm z $(1, 1)$ na (i, j).

Jednou z možností, jak definovat $\mathbb{N} \times \mathbb{N}$, je tato:

(0) $(1, 1) \in M$.

(1a) Jestliže $(i, 1) \in M$, tak $(i + 1, 1) \in M$.

(1b) Jestliže $(i, j) \in M$, tak $(i, j + 1) \in M$.

Rozmyslete si, že těmito pravidly dostanete libovolnou dvojici $(i, j) \in \mathbb{N} \times \mathbb{N}$. Princip strukturální indukce pak dovoluje důkaz vlastnosti V provést následujícími kroky:

(0) Platí $V(1, 1)$.

(1a) Jestliže platí $V(i, 1)$, pak platí $V(i + 1, 1)$.

(1b) Jestliže platí $V(i, j)$, pak platí $V(i, j + 1)$.

Zajímavou shodou okolností jsme přesně tato tvrzení dokázali v řešení 1), takže i onen důkaz šlo prezentovat jako strukturální indukci.

Jsou i jiné možnosti, jak zavést $\mathbb{N}^2$. Jak příklad uvedeme následující definici.

(0) $(1, 1) \in M$.

(1) Jestliže $(m, n) \in M$, tak $(m + 1, n) \in M$ a $(m, n + 1) \in M$.

Strukturální indukce pak vede na řešení, které odpovídá důkazům z 2) a 3).

△

Poznámka: Máme několik důkazů pro šachovnici nekonečnou, zajímavá otázka je, zda se s koněm dokážeme dostat na libovolné pole šachovnice konečné. Kritickým faktorem bude, zda máme dost místa na tahy nutné k provedení kroků indukce. Podíváme se na první důkaz. Pokud se chceme posunout o jedno pole doprava, pak naše tři tahy vyžadují alespoň dvě řady navíc směrem nahoru a jeden sloupec navíc směrem doprava. Pokud není místo vpravo, tak máme možnost jít v druhém tahu doleva, zase budeme potřebovat jeden sloupec navíc. Podobně k posunu nahoru potřebujeme alespoň dva sloupce nalevo či napravo a jednu řadu navíc nad či pod.

Po kratší úvaze lze dojít k závěru, že důkaz indukcí bude fungovat vždy, když má šachovnice alespoň 4 řady a sloupce.

Zbývají případy šachovnic 1×1, 2×2 a 3×3, které již snadno prozkoumáme kratší prací s tužkou a papírem. Zjistíme, že případ $n = 1$ je triviální a v případech $n = 2$ a $n = 3$ se nedokážeme dostat na pole $(2, 2)$. Nakonec tedy máme úplnou informaci, víme, že u všech velikostí šachovnic (včetně nekonečné) s výjimkou 2×2 a 3×3 se kůň dokáže dostat kamkoliv.

△

Výklad indukce teď zakončíme slíbeným důkazem ekivalence principů.

Věta 5b.3.
Platnost principu strukturální indukce je ekvivalentní platnosti principu matematické indukce.

Důkaz (drsný)**:** 1) Nejprve ukážeme, že slabý princip indukce plyne ze strukturální indukce.

Uvažujme tedy nějakou vlastnost $V(n)$ celých čísel, která má smysl pro $n \geq n_0$ a splňuje tyto podmínky:

(s0) $V(n_0)$ platí.

(s1) Pro všechna $n \geq n_0$ platí implikace: $V(n)$ platí $\implies$ $V(n + 1)$ platí.

Ukážeme, že když předpokládáme platnost strukturální indukce, tak V platí pro všechna $n \geq n_0$. Uvažujme množinu M definovanou předpisy

(0) $n_0 \in M$.

(1) $n \in M \implies n+1 \in M$.

Pak $M \subseteq \mathbb{Z}$, proto má V smysl pro prvky M. Předpoklad (s0) ukazuje, že V je splněna pro všechny prvky ze základního pravidla (0). Předpoklad (s1) ukazuje, že když je V splněna pro nějaký prvek z předpokladu induktivního pravidla (1), pak je splněna i pro prvek z jeho závěru. V tedy splňuje předpoklady principu strukturální indukce, proto podle něj V platí pro všechny prvky M, přičemž evidentně $M = \{n \in \mathbb{Z};\ n \geq n_0\}$. Proto $V(n)$ platí pro všechna $n \geq n_0$.

2) Teď ukážeme, že princip strukturální indukce plyne ze silného principu matematické indukce. Uvažujme tedy nějakou množinu M danou základními pravidly $(0i)$ a induktivními 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 induktivního pravidla. Vezměme si tedy jeho derivační strom, který dává výšku $n+1$, a vidíme, že m vzniklo použitím nějakého induktivního 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) i (S1), proto podle silného principu matematické indukce $W(n)$ platí pro všechna n, tedy V platí pro všechny prvky M.

□

Cvičení

Cvičení 5b.1 (rutinní)**:** Najděte $f(1)$, $f(2)$, $f(3)$, $f(4)$ pro f definované indukcí jako

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

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

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

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

Cvičení 5b.2 (rutinní)**:** Najděte $f(2)$, $f(3)$, $f(4)$ pro f definované indukcí jako

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

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

(iii) (0) $f(0) = 1$, $f(1) = -2$, (1) $f(n+1) = \frac{f(n-1)}{f(n)}$ pro $n \in \mathbb{N}$.

Cvičení 5b.3 (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.

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

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

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

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

(v) (0) $f(1) = 1$, $f(2) = 1$, $f(3) = 1$, (1) $f(n+1) = f(n) + f(n-1) - f(n-2)$ pro $n \in \mathbb{N}$, $n \geq 3$;

(vi) (0) $f(1) = 1$, $f(2) = 0$, $f(3) = 1$, (1) $f(n+1) = f(n) + f(n-1) - f(n-2)$ pro $n \in \mathbb{N}$, $n \geq 3$;

(vii) (0) $f(0) = 1$, $f(1) = 3$, (1) $f(n+1) = \begin{cases} 3f(n), & n \in \mathbb{N} \text{ liché;} \\ 9f(n-1), & n \in \mathbb{N} \text{ sudé;} \end{cases}$

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

(ix) (0) $f(0) = 1$, $f(1) = 0$, $f(2) = 2$, (1) $f(n) = 2f(n-3)$ pro $n \in \mathbb{N}$, $n \geq 3$.

Cvičení 5b.4 (rutinní, zkouškové)**:** Uvažujte funkce definované induktivně následujícími vzorci. Pro každou z nich dokažte zadanou (ne)rovnost.
(i) (0) $f(1)=1$, $f(2)=2$, (1) $f(n+1)=f(n)+n\,f(n-1)$ pro $n\geq 2$; nerovnost $f(n)\leq n!$;
(ii) (0) $f(1)=1$, $f(2)=2$, (1) $f(n+1)=\frac{1}{n}f(n)+f(n-1)$ pro $n\geq 2$; nerovnost $f(n)\leq n^2$;
(iii) (0) $f(1)=1$, $f(2)=2$, (1) $f(n+1)=n\,f(n)+n\,f(n-1)$ pro $n\geq 2$; rovnost $f(n)=n!$;
(iv) (0) $f(1)=2$, $f(2)=3$, (1) $f(n+1)=n\,f(n)+n^2 f(n-1)$ pro $n\geq 2$; nerovnost $f(n)\geq n!$.

Cvičení 5b.5 (rutinní, poučné)**:** Uvažujme posloupnost danou předpisem
(0) $F_1=F_2=1$.
(1) $F_{n+1}=F_n+F_{n-1}$ pro $n\geq 2$.
(Je to tzv. Fibonnaciho posloupnost, viz příklad 9a.c.)
a) Odhadněte, která F_n jsou lichá, a dokažte to.
b) Dokažte následující vztahy:
(i) $F_1^2+F_2^2+\cdots+F_n^2=F_nF_{n+1}$ pro $n\in\mathbb{N}$;
(ii) $F_1+F_3+\cdots+F_{2n-1}=F_{2n}$ pro $n\in\mathbb{N}$;
(iii) $F_{n+1}F_{n-1}-F_n^2=(-1)^n$ pro $n\in\mathbb{N}$;
(iv) $F_1F_2+\cdots+F_{2n-1}F_{2n}=F_{2n}^2$ pro $n\in\mathbb{N}$;
(v) $F_1-F_2+\cdots+F_{2n-1}-F_{2n}=1-F_{2n-1}$ pro $n\in\mathbb{N}$;
(vi) $F_kF_n+F_{k+1}F_{n+1}=F_{n+k+1}$ pro $n,k\in\mathbb{N}$;
(vii) $\begin{pmatrix}1&1\\1&0\end{pmatrix}^n=\begin{pmatrix}F_{n+1}&F_n\\F_n&0\end{pmatrix}$ pro $n\in\mathbb{N}$.

Cvičení 5b.6 (poučné, zkouškové)**:** Definujte množinu všech binárních slov, která:
(i) neobsahují více nul jdoucích po sobě;
(ii) končí nulou;
(iii) nekončí nulou;
(iv) obsahují někde v sobě kombinaci 101.

Cvičení 5b.7 (poučné, zkouškové)**:** Definujte množinu všech slov nad abecedou $C=\{1,2,3,4\}$, která:
(i) neobsahují více trojek jdoucích po sobě;
(ii) začínají dvojkou;
(iii) nekončí jedničkou;
(iv) obsahují stejný počet sudých a lichých číslic.

Cvičení 5b.8 (poučné)**:** Napište nějakou rekurzivní definici správných množinových výrazů složených z velkých písmen, $\cap$, $\cup$, $-$, $\overline{\ }$ a závorek.

Cvičení 5b.9 (poučné, zkouškové)**:** Napište nějakou rekurzivní definici množiny M všech slov nad anglickou abecedou C (26 malých písmen), které jsou palindromy, tj. čtou se stejně zleva doprava a zprava doleva.

Cvičení 5b.10 (poučné)**:** Napište nějakou rekurzivní definici množiny všech polynomů s reálnými koeficienty.
Nápověda: Indukce může zvyšovat stupeň.

Cvičení 5b.11 (poučné, dobré)**:** Napište rekurzivní definice těchto množin:
(i) $M=\{(a,b)\in\mathbb{N}\times\mathbb{N};\ a+b \text{ liché}\}$;
(ii) $M=\{(a,b)\in\mathbb{N}\times\mathbb{N};\ a\,|\,b\}$;
(iii) $M=\{(a,b)\in\mathbb{N}\times\mathbb{N};\ a \text{ nebo } b \text{ liché}\}$.
Dokažte, že vaše definice jsou správné.

Cvičení 5b.12 (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 5b.13 (poučné, zkouškové)**:** Uvažujte množinu čísel M definovanou induktivně takto:
(s0) $23\in M$.
(s1) $m\in M \implies 13\cdot m\in M$.
Dokažte, že $M=\{n\in\mathbb{N};\ \exists k\in\mathbb{N}_0\colon n=23\cdot 13^k\}=\{23\cdot 13^k,\ k\in\mathbb{N}_0\}$.

Cvičení 5b.14 (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 5b.15 (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:
5b.1: (i): $f(1) = f(0)+2 = 3$, $f(2) = f(1)+2 = 5$, $f(3) = 7$, $f(4) = 9$; (ii): $f(1) = 3f(0) = 3$, $f(2) = 3f(1) = 9$, $f(3) = 27$, $f(4) = 81$; (iii): $f(1) = f(0)^2 + f(0) + 1 = 3$, $f(2) = f(1)^2 + f(1) + 1 = 13$, $f(3) = 183$, $f(4) = 33673$; (iv): $f(1) = 2^{f(0)} = 2$, $f(2) = 2^{f(1)} = 4$, $f(3) = 16$, $f(4) = 65536$.
5b.2: (i): $f(2) = f(0)^2 f(1) = -2$, $f(3) = f(1)^2 f(2) = -8$, $f(4) = -32$; (ii): $f(2) = f(0) - 2f(1) = 5$, $f(3) = f(1) - 2f(2) = -12$, $f(4) = 29$; (iii): $f(2) = \frac{f(0)}{f(1)} = -\frac{1}{2}$, $f(3) = \frac{f(1)}{f(2)} = 4$, $f(4) = -\frac{1}{8}$.
5b.3: (i): $f(n) = 0$. Slabý princip. (0) $n = 0$ funguje. (1) Nechť $n \in \mathbb{N}_0$. Předpokládejme, že $f(n) = 0$. Pak $f(n+1) = 2f(n) = 0$, souhlasí pro $n+1$.
(ii): $f(n) = n-1$. Slabý princip. (0) $n = 1$ funguje. (1) Nechť $n \in \mathbb{N}$. Předpokládejme, že $f(n) = n-1$. Pak $f(n+1) = f(n)+1 = n-1+1 = (n+1)-1$, souhlasí pro $n+1$.
(iii): $f(n) = \frac{1}{n}$. Slabý princip. (0) $n = 1$ funguje. (1) Nechť $n \in \mathbb{N}$. Předpokládejme, že $f(n) = \frac{1}{n}$. Pak $f(n+1) = f(n)\frac{n}{n+1} = \frac{1}{n}\frac{n}{n+1} = \frac{1}{n+1}$, souhlasí pro $n+1$.
(iv): $f(n) = n$. Modifikovaný princip. (0) $n = 1$ a $n = 2$ funguje. (1) Nechť $n \in \mathbb{N}$. Předpokládejme, že $f(k) = k$ pro $k = n-1, n$. Pak $f(n+1) = 2f(n) - f(n-1) = 2n - (n-1) = n+1$, souhlasí pro $n+1$.
(v): $f(n) = 1$. Modifikovaný princip. (0) $n = 1$, $n = 2$ a $n = 3$ funguje. (1) Nechť $n \in \mathbb{N}$. Předpokládejme, že $f(k) = 1$ pro $k = n-2, n-1, n$. Pak $f(n+1) = f(n) + f(n-1) - f(n-2) = 1+1-1 = 1$, souhlasí pro $n+1$.
(vi): $f(n) = \begin{cases} 1, & n \text{ liché;} \\ 0, & n \text{ sudé.} \end{cases}$ Modifikovaný princip: (0) Pro $n = 1,2,3$ to funguje.
(1) Nechť $n \in \mathbb{N}$, $n \geq 3$. Předpokládejme, že $f(k) = \begin{cases} 1, & k \text{ liché;} \\ 0, & k \text{ sudé} \end{cases}$ pro $k = n-2, n-1, n$.
a) Je-li n sudé, pak $n-2$ je sudé, zato $n-1$ a $n+1$ jsou liché. Pak $f(n+1) = f(n)+f(n-1)-f(n-2) = 0+1-0 = 1$, souhlasí pro liché $n+1$.
b) Je-li n liché, pak $n-2$ je liché, zato $n-1$ a $n+1$ jsou sudé. Pak $f(n+1) = f(n)+f(n-1)-f(n-2) = 1+0-1 = 0$, souhlasí pro sudé $n+1$.
Alternativa: $f(n) = \frac{1}{2}(1-(-1)^n)$, pak lze přímo, z indukčního předpokladu vyjde
$f(n+1) = f(n) + f(n-1) - f(n-2) = \frac{1}{2}(1-(-1)^n) + \frac{1}{2}(1-(-1)^{n-1}) - \frac{1}{2}(1-(-1)^{n-2}) =$
$= \frac{1}{2}(1-(-1)^n + 1 + (-1)^n - 1 + (-1)^n) = \frac{1}{2}(1+(-1)^n) = \frac{1}{2}(1-(-1)^{n+1})$.
(vii): $f(n) = 3^n$. Modifikovaný princip. (0) $n = 1$ a $n = 2$ funguje. (1) Nechť $n \in \mathbb{N}$. Předpokládejme, že $f(k) = 3^k$ pro $k = n-1, n$. Uvažujme $n+1$.
Je-li $n+1$ sudé, pak $f(n+1) = 9f(n-1) = 9 \cdot 3^{n-1} = 3^{n+1}$.
Je-li $n+1$ liché, pak $f(n+1) = 3f(n) = 3 \cdot 3^n = 3^{n+1}$.
(viii): $f(n) = 2^{\lfloor n/2 \rfloor}$. Modifikovaný princip. (0) $n = 1$ a $n = 2$ funguje. (1) Nechť $n \in \mathbb{N}$. Předpokládejme, že $f(k) = \begin{cases} 2^{k/2}, & k \text{ sudé;} \\ 2^{(k-1)/2}, & k \text{ liché} \end{cases}$ pro $k = n-1, n$. Uvažujme $n+1$.
Je-li $n+1$ sudé, pak je i $n-1$ sudé a $f(n+1) = 2f(n-1) = 2 \cdot 2^{(n-1)/2} = 2^{(n+1)/2}$.
Je-li $n+1$ liché, pak je i $n-1$ liché a $f(n+1) = 2f(n-1) = 2 \cdot 2^{(n-1-1)/2} = 2^{n/2} = 2^{((n+1)-1)/2}$.
(ix): Jak zapsat $1,0,2,2,0,4,4,0,8,8,0,16,16,0,\ldots$? Nápad: $f(n) = \begin{cases} 0, & n = 3k+1; \\ 2^{\lfloor (n+1)/3 \rfloor}, & n \neq 3k+1. \end{cases}$
Důkaz modifikovanou indukcí podobný předchozímu, ale teď se musí řešit tři případy.
5b.4: (i): Modifikovaná indukce (0) Pro $n = 1,2$ to platí. (1) Nechť $n \geq 2$, předpoklad platnosti $V(k)$: $f(k) \leq k!$ pro $k = n-1, n$. Pak $f(n+1) = f(n) + n\,f(n-1) \leq n! + n \cdot (n-1)! = 2n! \leq (n+1)n! = (n+1)!$.
(ii): Modifikovaná indukce (0) Pro $n = 1,2$ to platí. (1) Nechť $n \geq 2$, předpoklad platnosti $V(k)$: $f(k) \leq k^2$ pro $k = n-1, n$. Pak $f(n+1) = \frac{1}{k}f(n) + f(n-1) \leq \frac{1}{n}n^2 + (n-1)^2 = n + n^2 - 2n + 1 = n^2 - n + 1 \leq n^2 + 2n + 1 = (n+1)^2$.
(iii): Modifikovaná indukce (0) Pro $n = 1,2$ to platí. (1) Nechť $n \geq 2$, předpoklad platnosti $V(k)$: $f(k) = k!$ pro $k = n-1, n$. Pak $f(n+1) = n\,f(n) + n\,f(n-1) = n \cdot n! + n \cdot (n-1)! = n \cdot n! + n! = (n+1) \cdot n! = (n+1)!$.

(iv): Modifikovaná indukce (0) Pro $n = 1, 2$ to platí. (1) Nechť $n \geq 2$, předpoklad platnosti $V(k)$: $f(k) \geq k!$ pro $k = n-1, n$. Pak $f(n+1) = n\,f(n)+n^2 f(n-1) = n\cdot n!+n^2\cdot(n-1)! = n\cdot n!+n\cdot n! = 2n\cdot n! \geq (n+1)\cdot n! = (n+1)!$.
5b.5: a): F_{3n} sudé, F_{3n+1} a F_{3n+2} liché. Důkaz najednou indukcí: (0) $n = 0$ funguje, pokud doplníme $F_0 = 0$. (1) Předpoklad: $n \in \mathbb{N}_0$ a F_{3n} sudé, F_{3n+1} a F_{3n+2} liché.
Pak $F_{3(n+1)} = F_{3n+3} = F_{3n+2} + F_{3n+1}$. Protože jsou dle indukčního předpokladu F_{3n+2} a F_{3n+1} liché, je $F_{3(n+1)}$ sudé.
Dále $F_{3(n+1)+1} = F_{3n+4} = F_{3n+3} + F_{3n+2}$. Protože je dle indukčního předpokladu F_{3n+2} liché a již jsme dokázali, že F_{3n+3} je sudé, je $F_{3(n+1)+1}$ liché.
Dále $F_{3(n+1)+2} = F_{3n+5} = F_{3n+4} + F_{3n+3}$. Protože jsme dokázali, že F_{3n+4} je liché a F_{3n+3} je sudé, je $F_{3(n+1)+2}$ liché.
b) (i): Slabá indukce: (0) $n = 1$ funguje, $1^2 = 1 \cdot 1$.
(1) Předpoklad: Platí to pro jisté $n \in \mathbb{N}$. Pak
$F_1^2 + F_2^2 + \cdots + F_{n+1}^2 = [F_1^2 + F_2^2 + \cdots + F_n^2] + F_{n+1}^2 = F_n F_{n+1} + F_{n+1}^2 = F_{n+1}(F_n + F_{n+1}) = F_{n+1}F_{n+2}$.
Zbytek podobně.
5b.6: (i): (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 101.
(ii): (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.
(iii): (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.
(iv): (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) $w \in M \implies w1 \in M$.
5b.7: (i): (0a) $c \in C \implies c \in M$. (0b) $c \in C - \{3\} \implies c3 \in M$.
(1a) $[w \in M \wedge c \in C - \{3\}] \implies wc \in M$. (1b) $[w \in M \wedge c \in C - \{3\}] \implies wc3 \in M$.
Poznámka: Bez (0b) nelze získat 13.
(ii): (0) $2 \in M$. (1) $[w \in M \wedge c \in C] \implies wc \in M$.
(iii): (0) $c \in C - \{1\} \implies c \in M$. (1) $[w \in M \wedge c \in C] \implies cw \in M$.
Poznámka: Nutno přidávat nalevo, zprava nejde zaručit správné ukončení.
(iv): (0a) $\lambda \in M$ (0b) $[c \in \{1,3\} \wedge d \in \{2,4\}] \implies cd \in M$. (0c) $[c \in \{1,3\} \wedge d \in \{2,4\}] \implies dc \in M$.
(1a) $[r, s \in M \wedge c \in \{1,3\} \wedge d \in \{2,4\}] \implies rcsd \in M$. (1b) $[r, s \in M \wedge c \in \{1,3\} \wedge d \in \{2,4\}] \implies rdsc \in M$.
Poznámka: Přidáváme napravo, vždy někam doprostřed vsuneme číslo opačné parity. Je to dobře? Úvaha přes rekurentní postup, od daného řetězce vždy odebereme pravý krajní znak a s ním i nějaký znak opačné parity ze zbytku řetězce. Je pak nutné umožnit odebírání zevnitř, viz řetězec 11222211, ale lze se obejít bez odebírání z druhého kraje. Má-li řetězec alespoň 4 znaky, pak v něm musí existovat alespoň dva znaky parity opačné než je ta na pravém konci, tudíž alespoň jeden znak správné parity je někde uprostřed a dá se odebrat.
Podmínku (0a) jsme museli přidat, jinak bychom nedokázali vytvořit třeba 1122.
5b.8: (0) $A, B, \ldots, Z \in \mathcal{M}$.
(1a) $v \in \mathcal{M} \implies \overline{v} \in \mathcal{M}$. (1c) $v_1, v_2 \in \mathcal{M} \implies (v_1 \cup v_2) \in \mathcal{M}$.
(1b) $v_1, v_2 \in \mathcal{M} \implies (v_1 \cap v_2) \in \mathcal{M}$. (1d) $v_1, v_2 \in \mathcal{M} \implies (v_1 - v_2) \in \mathcal{M}$.
5b.9: (0a) $c \in C \implies c \in M$. (0b) $c \in C \implies cc \in M$.
(1) $[w \in M \wedge c \in C] \implies cwc \in M$.
5b.10: (0) $a \in \mathbb{R} \implies a \in P$. (1) $[p \in P \wedge a \in \mathbb{R}] \implies x \cdot p + a \in P$.
Alternativa (méně elegantní): (1) $[p \in P \wedge a \in \mathbb{R} \wedge n \in \mathbb{N}] \implies p + ax^n \in P$.
Poznámka: Proč by nefungovala definice (1) $[p \in P \wedge a \in \mathbb{R}] \implies (x - a) \cdot p \in P$? Což takhle $x^2 + 1$?
5b.11: (i): (0) $(2, 0) \in S$, $(2, 1) \in S$.
(1a) $(a, b) \in S \implies (a + 2, b) \in S \in S$. (1b) $(a, b) \in S \implies (a, b + 2) \in S$.
a) $S \subseteq M$ strukturální indukcí: (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 $(a, b + 2) \in M$.
b) $M \subseteq S$ nejlépe silnou indukcí 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 $a + b = 1$, pak z $a, b \in \mathbb{N}_0$ plyne, že $(a, b) = (1, 0)$ nebo $(a, b) = (0, 1)$, každopádně dle (0) v definici $(a, b) \in S$.

(1) Předpokládáme platnost pro jisté $n \in \mathbb{N}$. Nechť $(a,b) \in \mathbb{N}_0^2$ 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.
(ii): (0) $(1,1) \in S$.
(1a) $[(a,b) \in S \wedge c \in \mathbb{N}] \implies (ac,bc) \in S$. (1b) $[(a,b) \in S \wedge c \in \mathbb{N}] \implies (a,bc) \in S$.
a) $S \subseteq M$ lehce strukturální indukcí. a b) $M \subseteq S$ nejlépe ve dvou krocích. V prvním kroku indukcí na a dokázat, že $(a,a) \in S$. V druhém kroku silnou indukcí na $\frac{b}{a}$ dokázat $M \subseteq S$.
(iii): (0) $(1,1) \in S$, $(1,2) \in S$, $(2,1) \in S$.
(1a) $(a,b) \in S \implies (a+2,b) \in S$. (1b) $(a,b) \in S \implies (a,b+2) \in S$.
a) $S \subseteq M$ lehce strukturální indukcí. b) $M \subseteq S$ nejlépe silnou indukcí 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.

5b.12: Uvažujme $f(r)$ na M udávající počet znaků a v řetězci r. Dokážeme, že f má v M sudé hodnoty.
Silná indukce. (0) V pravidle (d0) 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.

5b.13: Dvě inkluze
1) $W(k)$: $23 \cdot 13^k \in M$ indukcí (slabým principem):
(0) $k = 0$: $23 \cdot 13^0 = 23 \in M$ dle (s0).
(1) $k \in \mathbb{N}_0$, nechť $W(k)$ platí, tedy $23 \cdot 13^k \in M$. Pak podle (s1) je v M i $13 \cdot 23 \cdot 13^k = 23 \cdot 13^{k+1}$, 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 indukcí, 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 induktivního 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 $M \subseteq \{23 \cdot 13^k;\ k \in \mathbb{N}_0\}$.

5b.14: Definujme množinu $M = \mathbb{N}_0^2$ strukurální indukcí takto:
(d0): $(0,0) \in M$.
(d1a): $(m,0) \in M \implies (m+1,0) \in M$.
(d1b): $(m,n) \in M \implies (m,n+1) \in M$.
Vlastnost $V(m,n)$ na množině M: pro $(m,n) \in M$ platí $a(m,n) = m+n$. Platnost dokážeme strukturální indukcí 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 $(m,n+1)$.

5b.15: (1b) $a(m,n+1) = a(m,n)+2$ pro $m,n \in \mathbb{N}$
splňují $a(m,n) = 2(m+n)+1$ pro $m,n \in \mathbb{N}$.
Definujme množinu $M = \mathbb{N}^2$ strukurální indukcí takto:
(d0): $(1,1) \in M$.
(d1a): $(m,1) \in M \implies (m+1,1) \in M$.
(d1b): $(m,n) \in M \implies (m,n+1) \in M$.
Vlastnost $V(m,n)$ na množině M: pro $(m,n) \in M$ platí $a(m,n) = 2(m+n)+1$. Platnost dokážeme strukturální indukcí dle definice M:
(0) Pro prvek $a(1,1) = 5$ to platí.
(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 $(m,n+1)$.