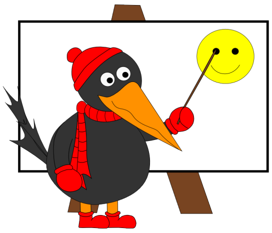
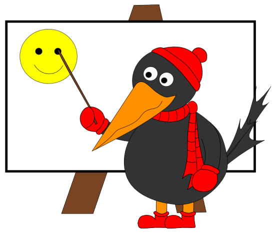


Pomocný text

INVARIANTY



Invarianty – o co jde

Slovo invariant můžeme přeložit do češtiny jako „neměnek“, je to tedy něco, co se nemění. Typické zadání úlohy, ve které můžeme invariant použít, většinou obsahuje nějaký začáteční stav a operaci, kterou s ním můžeme udělat. Úkolem pak bývá zjistit, do jakých stavů se pomocí této operace můžeme či nemůžeme dostat.

Metoda použití invariantu spočívá v tom, že najdeme nějakou vlastnost stavů, kterou daná operace zachovává. Pokud má tuto vlastnost počáteční stav, budou ji mít všechny dosažitelné stavy. Metoda je tedy vhodná pro dokázání, že nějakého stavu nelze dosáhnout. Ukažme si to na příkladu:

Příklad 5.1. Mějme množinu čísel $\{3, 4, 12\}$. V každém kroku z ní vezmeme nějaká dvě čísla a, b a nahradíme je čísly $0.8a + 0.6b$, $0.6a - 0.8b$. Je možné opakováním této operace získat množinu $\{4, 6, 12\}$?

Uvažujme součet druhých mocnin čísel v množině a sledujme, co s ním provede daná operace.

$$\begin{aligned}&(0.8a + 0.6b)^2 + (0.6a - 0.8b)^2 + c^2 = \\ &\qquad = 0.64a^2 + 0.48ab + 0.36b^2 + 0.36a^2 - 0.48ab + 0.64b^2 + c^2 = a^2 + b^2 + c^2\end{aligned}$$

Operace tedy nezmění součet druhých mocnin. Z množiny $\{3, 4, 12\}$ proto nemůžeme přejít na žádnou množinu, jejíž součet druhých mocnin není $3^2 + 4^2 + 12^2 = 169$. Jelikož $4^2 + 6^2 + 12^2 = 196$, odpověď zní ne.

Následuje několik příkladů, co lze například považovat za invariant:

- Parita čísla je invariantní při násobení lichým číslem.
- Ciferný součet. Při operaci ciferného součtu zůstává stejný zbytek po dělení 9. Z tohoto invariantu vychází kritérium pro dělitelnost 9, které jistě znáte.
- Mocnost bodu ke kružnici. Mějme v rovině kružnici k a bod A. Veďme bodem A přímku p, která protíná kružnici k v bodech P, Q. Pak součin $|AP| \cdot |AQ|$ nezávisí na volbě přímky.
- Eulerova formule. Mějme rovinný graf s v vrcholy, e hranami a f stěnami. Pak platí $v + f = e + 2$.

BRKOS Team 2011

V posledních dvou příkladech není žádná transformace stavu. Jedná se ale o hodnotu, která je nezávislá na volbě přímek, resp. struktury grafu, pročež si rozhodně zaslouží označení „invariant“.

Monovarianty

To, že operace opravdu zachovává nějakou hodnotu, je spíše ojedinělý jev. Často tedy při hledání invariantu budeme neúspěšní. Naštěstí není třeba se omezovat jen na hodnoty, které se nemění. Mnoho nám prozradí i hodnoty, které se mění nějak pravidelně.

Myšlenka monovariantu je zobecnění invariantů – hledáme hodnoty, které operace mění monotónně. Pokud např. najdeme ohodnocení stavů, které při operaci neroste, dokážeme tím nedosažitelnost stavů s vyšším ohodnocením než měl počáteční stav. Pokud se nám povede nalézt ohodnocení, které vždy klesá alespoň o nějaké číslo $\varepsilon > 0$, počáteční stav nechť má ohodnocení a_0, cílový $a_1 < a_0$, můžeme tvrdit, že se do cílového stavu dostaneme nejvýše po $\frac{a_0 - a_1}{\varepsilon}$ krocích. Podobných použití je mnohem víc, záleží co úloha vyžaduje.

Ukažme si použití na ilustračním příkladu:

Příklad 5.2. Mějme čtvercovou tabulku $n \times n$, jejíž některá pole jsou na začátku vybarvená černě. V každém kroku vybereme bílé políčko, které má alespoň 2 černé sousedy (hranou) a začerníme ho. Dokažte, že pokud je na začátku $n - 1$ černých polí, není možné, aby se po konečném počtu kroků začernila celá tabulka.

Dokázat něco takového není žádná legrace, přestože to intuitivně je docela jasné. Sledujme, co se při začernění děje se **součtem obvodů černých oblastí**. Pokud pole sousedí alespoň s dvěma černými, nejméně dvě hrany z obvodu ubydou, zatímco nejvýše dvě přibudou. Součet obvodů černých oblastí tedy neroste. Pro $n - 1$ polí je na začátku obvod nejvýše $4(n - 1)$, zatímco pro celou černou tabulku by byl $4n$, což je spor.

Invarianty a monovarianty mohou vypadat velmi různorodě a nemá smysl se zabývat teorií, jak je hledat. Raději si je ukážeme na typických příkladech.

Příklady

Příklad 5.3. Na tabuli jsou napsaná čísla $1, 2, ..., 4n$. V každém kroku si náhodně vybereme dvě čísla na tabuli, smažeme je a připíšeme jejich rozdíl. Je možné, aby po několika krocích zbylo na tabuli pouze číslo 1?

Úloha se tedy vysloveně ptá na dosažitelnost nějakého stavu. Zadání tím přímo vybízí k využití invariantů a napovídá, že odpověď bude spíš **ne**. Jediné, co je potřeba, je podívat se na čísla modulo 2. Rozdíl lichého a lichého čísla, stejně tak jako sudého a sudého čísla, bude vždy sudý. Naopak rozdíl lichého a sudého bude vždy lichý. Počet lichých čísel na tabuli se tedy buď nezmění, nebo se zmenší o 2. Závěr tedy je, že **parita počtu lichých čísel** se nemění. Na začátku je lichých čísel zřejmě $2n$, počet lichých čísel tedy vždy bude sudý. Pokud zbyde na tabuli jediné číslo, musí být sudé. Invariant lze ekvivalentně formulovat i takto: parita součtu čísel na tabuli se nemění.

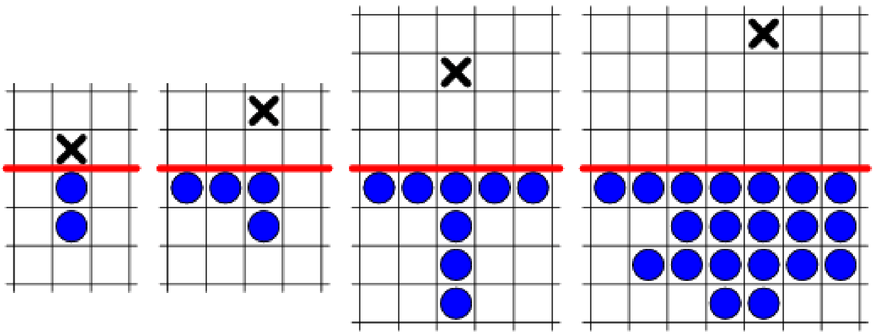
Příklad 5.4. Henry má 13 hrušek, 15 jablek a 17 švestek. Ochotná prodavačka mu nabídla, že mu dva různé kusy ovoce vymění za dva kusy ovoce třetího druhu. Je možné, aby Henry pomocí několika výměn získal 45 kusů stejného druhu ovoce?

Zde už se invariant trochu schoval. Pozorujme, jak se mění rozdíl mezi počtem dvou druhů. Pokud vyměňujeme tyto dva druhy za třetí, rozdíl se nemění. V opačném případě se počet jednoho druhu o 1 sníží a počet druhého o 2 zvýší. Rozdíl se tedy změní o 3. Všechny tři vzájemné rozdíly mezi počty druhů jsou proto invariantní modulo 3. Pokud by měl na konci 45 druhů jednoho ovoce, musely by být dva rozdíly dělitelné třemi, což na začátku nejsou. Není to možné.

Příklad 5.5. (Conwayovi vojáci)

Henry našel na půdě nekonečně velkou šachovnici. Rozhodl se, že si zahraje cosi jako dámu, ale upravil pravidla tak, aby velkou šachovnici využil a stačily mu jen figurky jedné barvy. Povolený tah je přeskočit kámen na sousedním poli, je-li za ním volno. Tím se přeskakující kámen přesouvá a přeskakovaný umírá. Dále si na šachovnici zvolil jednu přímku (hranici mezi poli) a nějaké své kameny naskládal na jednu stranu od ní. Nyní se snaží přeskákat co nejdále **za přímku**.

Do jaké největší vzálenosti od přímky může v konečném počtu tahů Henry doskákat, jestliže má dostatek kamenů a může je na začátku položit na libovolná místa (na zvolené straně od přímky)?



Na obrázku výše jsou nakreslené konfigurace, z nichž se dá dostat do vzdálenosti 1,2,3 a 4 od přímky (sami si zkuste najít posloupnosti tahů, které k tomu vedou). Nás ale bude zajímat, jak dokázat, že do vzdálenosti 5 se doskákat nedá.

Vyberme si cílové pole ve vzdálenosti 5 a přiřaďme mu hodnotu 1. Okolním čtyřem polím přiřadíme a, okolním okolních a^2 atd. Formálně pokud má tedy cílové pole souřadnice $[x_0, y_0]$, ohodnotíme pole $[x, y]$ číslem $a^{|x-x_0|+|y-y_0|}$. Celkové ohodnocení, které budeme chtít udělat monovariantní, bude součet ohodnocení polí, na kterých jsou kameny.

Rozeberme nyní možné tahy:

- Kladné tahy. Kámen skáče směrem k cílovému poli. V tomto případě skáče z pole x^n přes x^{n-1} na x^{n-2}. Změna ohodnocení tedy bude $a^{n-2} - a^{n-1} - a^n = a^{n-2}(1 - a - a^2)$.
- Neutrální tahy. Kámen si zachová vzdálenost od cílového pole. V takovém případě skáče z a^n přes a^{n+1} na a^n. Změna ohodnocení je $-a^n$.
- Záporné tahy. Kámen skáče směrem od cílového pole. V těchto případech skáče z a^n přes a^{n+1} na a^{n+2}. Změna ohodnocení je proto $a^{n+2} - a^{n+1} - a^n = a^n(a^2 - a - 1)$.

Díky neutrálním tahům určitě nedocílíme toho, aby ohodnocení neklesalo. Budeme tedy chtít, aby ohodnocení nerostlo. a musí být kladné, takže hledáme řešení soustavy nerovnic

$$\begin{aligned}(1 - a - a^2) &\leq 0\\ (a^2 - a - 1) &\leq 0\end{aligned}$$

Pokud v první nerovnici položíme rovnost, kladný kořen bude $a = \frac{1}{2}(1 + \sqrt{5})$. Zřejmě $a^2 - a - 1 \leq a^2 + a - 1 = 0$, máme tedy řešení.

Nyní se již můžeme pustit do počítání, jaké je maximální počáteční ohodnocení. Spočtěme ohodnocení stavu, kdy jsou kameny na všech polích pod přímkou. Součet prvního řádku je

$$S_1 = a^5 + 2(a^6 + a^7 + ...) = a^5 + \left(\frac{2a^6}{1 - a}\right) = \left(\frac{a^5 + a^6}{1 - a}\right)$$

Každý prvek v i. řádku je a násobek odpovídajícího prvku v $(i-1)$., takže pro součet i-tého řádku platí $S_i = aS_{i-1}$. Proto

$$S = \sum_{1}^{\infty} S_i = \frac{S_1}{1 - a} = \frac{a^5 + a^6}{(1 - a)^2}$$

Snadno nahlédneme, že $1 - a = a^2$, a tedy $S = a^1 + a^2 = 1$.

Díky správné volbě a ohodnocení v průběhu neroste. Dosažitelné stavy tedy mají ohodnocení nejvýše 1. Pokud by kámen šel dostat na cílové pole, bylo by ohodnocení tohoto stavu alespoň 1, muselo by tedy být právě 1 a byl by to jediný kámen na šachovnici. V tom případě by ale na začátku musely být opravdu všechna pole pod přímkou pokrytá. Nekonečně mnoho kamenů ale v konečně mnoha krocích neodstraníme. Po konečně mnoha krocích tedy nelze doskákat do vzdálenosti 5.

Závěrem si jen pro zajímavost ukažme příklad, který jste mohli potkat na loňské mezinárodní matematické olympiádě.

Příklad 5.6. V každé ze šesti schránek B_1, B_2, B_3, B_4, B_5 a B_6 je na počátku jedna mince. Se schránkami můžeme provádět následující dvě operace:

1. Vybrat neprázdnou schránku B_j , kde $1 \leq j \leq 5$, odebrat z ní jednu minci a přidat dvě mince do schránky B_{j+1}.

2. Vybrat neprázdnou schránku B_k , kde $1 \leq k \leq 4$, odebrat z ní jednu minci a navzájem vyměnit obsahy (případně prázdných) schránek B_{k+1} a B_{k+2}.

Rozhodněte, zda je možné pomocí konečného počtu těchto operací dosáhnout toho, aby schránky B_1, B_2, B_3, B_4 a B_5 byly prázdné a schránka B_6 obsahovala právě $2010^{2010^{2010}}$ mincí.

Typická úloha na invariant, nemáte pocit? Druhá operace je opravdu vypečená a hledání invariantu velmi komplikuje. Po hlubším zkoumání operací zjistíte, že operace nějakým způsobem pomalu přesouvají mince do schránek s vyššími čísly. Lze tedy usoudit, že nebude možné dostat do B_6 libovolně velké množství mincí. No a $2010^{2010^{2010}}$ je docela velké číslo[1], takže to nejspíš nepůjde.

Jenže chyba, možné to je. Dané množství mincí v poslední schránce získat lze, přestože libovolně velké množství možné není. Příslušný monovariant je ale poněkud nad rámec tohoto povídání.

To bylo jen na ukázku, že pokud dlouho nemůžete najít invariant, který by něco vyloučil, je dobré se zamyslet, jestli to náhodou není možné :-)

[1] má zhruba 10^{6640} cifer