

Kategorie mladší

Úloha 1A Závody

Pokusíme se určit celkové pořadí sedmi zvířátek ze čtyř závodů, kde v každém závodě soutěžila čtyři z nich. Zkusme vyjít z prvního závodu (s pořadím C, B, A, G) a doplnit do jeho pořadí zbývající zvířátka (D, E, F).

Ve druhém závodě soutěžila o proti prvnímu navíc zvířátko E a D. Zvířátko D skončilo až za zvířátkem G, které bylo poslední v prvním závodě. Můžeme tedy výsledky prvního závodu rozšířit na C, B, A, G, D.

Zvířátko E zatím tak jednoznačně zařadit nemůžeme. Víme, že je rychlejší než B, ale nevíme, jestli ho zařadit před C nebo až za C.

Ze třetího závodu se dozvídáme, že zvířátko E je pomalejší než C. E je tedy rychlejší než B a pomalejší než C, takže rozšíříme původní pořadí na C, E, B, A, G, D. Chybí nám pouze zvířátko F, jehož pořadí zatím není jednoznačné.

Čtvrtý závod zvířátko F prohrálo proti zvířátku D, které bylo podle našeho pořadí dosud nejpomalejší. Tím pádem ho můžeme zařadit na konec. Dostaneme finální pořadí C, E, B, A, G, D, F.

Nejrychlejším zvířátkem je Cecilka, druhým nejrychlejším zvířátkem je Emanuel. Pořadí všech zvířátek lze jednoznačně určit, jak jsme si ukázali výše.

Úloha 2A Barevné bakterie

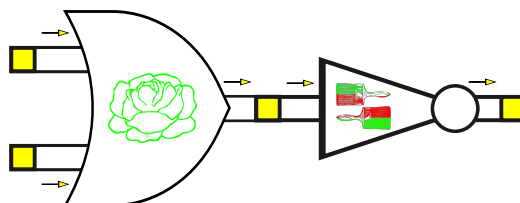
2.1 První úloha

Nejdříve zkusíme vymyslet první úlohu, kde potřebujeme vyrobit stroj vyrábějící zelenou bakterii ze dvou červených (a červenou z jakékoli jiné kombinace). Podle nápovědy by nám k tomu měly stačit dva přístroje. Jeden určitě nestačí, což vidí Mojmír s Metlou již v příslušných tabulkách.

1. vpuštěná bakterie	2. vpuštěná bakterie	vypuštěná bakterie
zelená	zelená	zelená
červená	zelená	zelená
zelená	červená	zelená
červená	červená	červená

Tabulka 1: Zelírna

Když se nicméně podíváme na vstupní a výstupní bakterie v tabulce zelírny, můžeme si povšimnout, že výstupní bakterie jsou přesně opačné oproti těm, které bychom chtěli, takže postačí, když na konec zelírny připojíme lakovnu a ta jim pokaždé barvu převrátí.



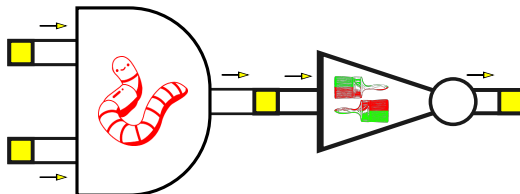
Obrázek 1: Řešení první úlohy

1. vpuštěná bakterie	2. vpuštěná bakterie	výstup Zelírny	vypuštěná bakterie
zelená	zelená	zelená	červená
červená	zelená	zelená	červená
zelená	červená	zelená	červená
červená	červená	červená	zelená

Tabulka 2: Řešení první úlohy

2.2 Druhá úloha

Nyní Mojmir s Metlou ví, že lakovna prohazuje bakterie na výstupu zelírny a to samé by nejspíše dokázali s červírnou. Tím bychom získali ve třech ze 4 případů zelenou vstupní bakterii, podobně jako v zelírně. Tabulka by pak vypadala následovně:

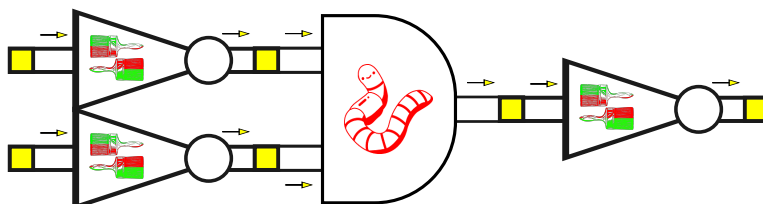


Obrázek 2: Řešení druhé úlohy - první krok

1. vpuštěná bakterie	2. vpuštěná bakterie	výstup Červírny	vypuštěná bakterie
zelená	zelená	zelená	červená
červená	zelená	červená	zelená
zelená	červená	červená	zelená
červená	červená	červená	zelená

Tabulka 3: Řešení druhé úlohy – první krok

Oproti zelírně, kterou se snaží vytvořit je zde však ještě jeden rozdíl. Ze dvou červených by měla vzniknout červená, nikoli zelená a ze dvou zelených zelená, nikoli červená. Toho můžeme dosáhnout jednoduše – stačí přebarvit obě vstupní bakterie v lakovně. Pokud budou na začátku od sebe odlišné, výslednou bakterii to nezmění. Pokud ale budou obě stejné, ze dvou červených vzniknou dvě zelené a ze dvou zelených dvě červené. Můžeme zkontrolovat tabulku a opravdu – vyrobili jsme zelírnu. Lakovny jsou číslovány odshora dolů, zleva doprava.



Obrázek 3: Řešení druhé úlohy - druhý krok

1. vpuštěná bakterie	2. vpuštěná bakterie	výstup 1. lakovny	výstup 2. lakovny	výstup Červírny	vypuštěná bakterie
zelená	zelená	červená	červená	červená	zelená
červená	zelená	zelená	červená	červená	zelená
zelená	červená	červená	zelená	červená	zelená
červená	červená	zelená	zelená	zelená	červená

Tabulka 4: Řešení druhé úlohy – druhý krok

2.3 K čemu to bylo?

Právě jste si vyzkoušeli práci s tzv. *logickými hradly*, které dnes najdete jako základní stavební kameny každé elektroniky, co něco počítá – v mobilech, počítačích, platební kartách, nebo i v utajené, dobře schované krabici, co ovládá semafor na cestě do školy.

Rozdíl je v tom, že místo dopravními trubičkami pomyslné bakterie putují dráty a červená bakterie v něm představuje **slabý až žádný elektrický signál** (nazýváme jako *logickou 0*), zelená bakterie **silný elektrický signál** (nazýváme jako *logickou 1*).

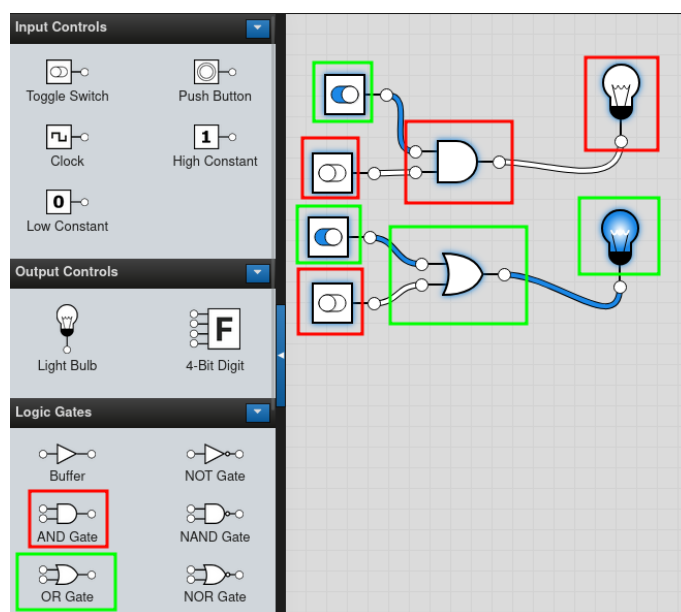
Pro přehlednost se ještě podívejme na to, jak se říká které součástce ve skutečnosti a co dělají:

- **Zelírnu** známe jako *OR hradlo* a propustí silný signál pokud dostane alespoň jeden silný signál (jedničku), jinak dále vysílá nulu.

- **Červírna** (AND hradlo) propustí jedničkový signál dál jenom když dostane dvě jedničky, jinak dále vysílá nulu.
- **Lakovna** značí tzv. NOT hradlo, nebo-li negaci (z jedničky dělá nulu a z nuly jedničku).
- **Množírna** je obyčejný rozdvojený drát, posílá signál beze změny do více směrů.
- **Dopravní trubičku** si můžeme představit jako obyčejný elektrický vodivý drát.

Už na některých středních školách se můžete naučit z takových součástek složit třeba jednoduché zařízení na sčítání, násobení... Zkrátka základní funkce, co počítače potřebují pro své fungování. Obvykle se k tomu používá soustava "Lakoven zapojených za zelírnu", chci říct AND+NOT hradla, nebo-li NAND hradlo. Ostatně, sami jste si takovou součástku vyrobili v první úloze.

Pokud byste si chtěli s hradly více pohrát, mohu doporučit například online stavebnici **Logic.ly** (<https://logic.ly/demo/>) a zapojit si jednotlivé součástky do sebe, jak se vám jen bude líbit. Že někudy teče silný jedničkový signál si můžete ověřit žárovkou. Tlačítka (Switch) potom simulují vyslání jedničky, pokud je stisknete, jinak vysílají nulu.



Obrázek 4: Logic.ly, pomyslné zelené bakterie a zelírna označeny zeleně, červené bakterie a červírna červeně

Úloha 3A Med-vědí banka – mladší

Podúloha i)

Jediná možná hesla jsou čísla od 0000 po 9999, kterých je přesně 10000 možných (4 číslice po 10 možnostech, celkem tedy $10 \cdot 10 \cdot 10 \cdot 10 = 10000$).

Pokud vosy dokážou každou sekundu zadat přesně 20 hesel, vyzkoušet všechna hesla jim potrvá maximálně $\frac{10000}{20} = 500$ sekund, tedy 8 minut a 20 sekund!

Poznámka bokem, k řešení není potřeba: Často se pro takové číslo používá zkrácený zápis $10 \cdot 10 \cdot 10 \cdot 10 = 10^4$ (deset na čtvrtou), protože násobíme po sobě čtyři desítky a nechce se nám je všechny vypisovat. Je to podobné, jako známe u násobení a sčítání – místo $10 + 10 + 10 + 10$ napíšeme $10 \cdot 4$. Pro čísla začínající na jedničku a pokračující pouze nulami navíc platí hezké pravidlo, že se rovná deseti právě „na tolikátou“, kolik má počet nul, takže $10 = 10^1$, $100 = 10^2$, $1000 = 10^3$ a tak dále.

Podúloha ii)

Pro každý znak hesla nyní existuje 62 možných hodnot (26 malých písmen, 26 velkých písmen a 10 číslic). Protože jednotlivé znaky nemohou ovlivnit jiné, jsou všechny pozice na sobě nezávislé. Celkový počet možných kombinací tak lze dostat tím, že se 62 vynásobí tolikrát, kolik má heslo znaků, nebo-li 62 se umocní na tolikátou, kolik znaků má heslo.

Protože musí existovat alespoň 1 000 000 000 000 (10^{12} , viz poznámka výše) možných hesel, je potřeba zjistit, na kolikátou umocnit základ 62, aby byl výsledek $\geq 1\,000\,000\,000\,000$.

Dopočítat se ke správné délce hesla můžeme tím, že budeme zkoušet pro kolik znaků je heslo dostatečně dlouhé. Jednoduše lze spočítat, že $62 \cdot 62 \cdot 62 \cdot 62 \cdot 62 \cdot 62 = 62^6 \doteq 5,6 \cdot 10\,000\,000\,000$ (přibližně), zatímco $62 \cdot 62 \cdot 62 \cdot 62 \cdot 62 \cdot 62 \cdot 62 = 62^7 \doteq 3,5 \cdot 1\,000\,000\,000\,000$ (přibližně), což již stačí. Takto lze tedy také zjistit, že Vendy si vytvoří nové heslo o délce 7 znaků.



Vosám zabere vyzkoušení všech možných hesel zhruba $3,5 \cdot 10\,000\,000\,000$ sekund, což je asi 1100 let. Vendy už může doufat, že je její heslo v bezpečí.

(Poznámka bokem: Pokud je někdo opravdu hodně vepředu s učivem a zná funkci zvanou logaritmus, může si spočítat, že $\log_{62} 10^{12} \doteq 6,7$ a je tedy potřeba alespoň 7 znaků dlouhé heslo. Tím se ale teď nemusíte trápit, logaritmy vás čekají až na střední škole a nikdo je po vás nebude chtít v tuto chvíli ani na Matematické olympiádě.)

Podúloha iii)

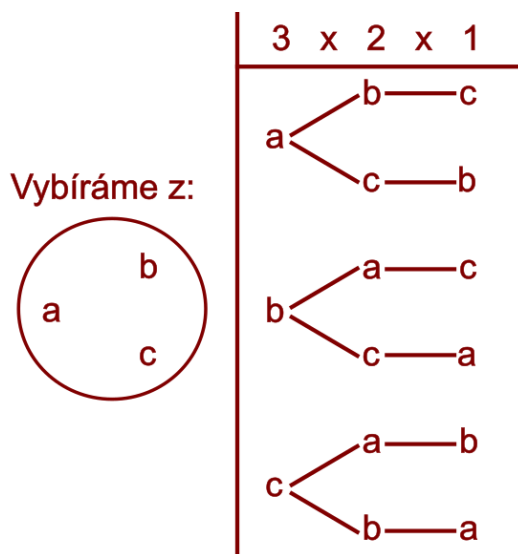
Vendy ví, ze kterých 7 znaků se heslo skládá, ale neví jejich pořadí. Pořadí 7 různých věcí lze spočítat tak, že na první pozici může být libovolný znak ze znaků, co si pamatuje. Na druhé už ale vybírá pouze z 6 možných znaků, protože první už si vybrala, ať už byl jakýkoli. Tím má vlastně vypsané všechny možné kombinace prvních dvou znaků hesla.

Na třetí jí tedy zbývá pokaždé už jen 5 zbylých možných znaků a takhle postupně získá všechna možná seřazení znaků (až na poslední pozici může být jen jeden přesně daný znak).

Celkový počet možných vyhovujících hesel tak je $7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5040$. Při variantě s 8 znaky je přesně 5040 způsobů, jak uspořádat posledních 7 znaků a 8 způsobů, jak vybrat první znak, celkem tedy $8 \cdot 5040 = 40320$.

Ostatně, že to funguje si můžete vyzkoušet sami na menším hesle:

- Napište si na papír pod sebe nejdříve třeba tři různé znaky **a**, **b**, **c**.
- Poté si za ně запиšte, jaké všechny znaky mohou být na první pozici: inu, buď **a**, nebo **b**, nebo **c**.
- Pokud už jste na začátku zvolili **a**, vedou z něj už jen dvě možnosti na to, jaký znak může být na druhé pozici – buď **b**, nebo **c** (a už máme na první). Obdobně pro druhou pozici u možných hesel začínajících na **b** nebo **c**.
- Na třetí a poslední pozici už nám vždycky zbude jen jeden znak, protože jsme pokaždé vybrali dva ze tří možných znaků z naší pomyslné hromádky.
- Možných hesel je tedy $3 \cdot 2 \cdot 1$.



Obrázek 5: Pořadí znaků hesla názorně

Podúloha iv)

Zde se počet možností bude počítat stejně jako v části ii), akorát místo s číslem 62 je potřeba počítat s číslem 314 159.

Budeme opět postupně násobit počet možností, jen ne pro jeden znak samostatně, ale pro počet slov (což je v našem případě 314 159). Pro dvě slova lze zjistit, že kombinací je $314\,159 \cdot 314\,159 = 314\,159^2 \doteq 9,9 \cdot 10\,000\,000\,000$, zatímco $314\,159 \cdot 314\,159 \cdot 314\,159 = 314\,159^3 \doteq 3,1 \cdot 10\,000\,000\,000\,000$. Takto lze také zjistit, že stačí tři slova.

Pro představu, pokud by vosy zkoušely všechny kombinace tří slov rychlostí 20 hesel za sekundu, trvalo by jim to necelých 50 000 000 let.

(Možným řešením pro silně pokročilé je i zde spočítat $\log_{314159} 10^{12} \doteq 2,2$, potřeba jsou tedy jen tři slova.)

Podúloha v)

V této úloze dostali bod prakticky všichni, kdo zkusili zauvažovat nad tím, jaké heslo by mohlo být bezpečnější a proč.



Jaká možnost je ale nakonec lepší? Náhodné znaky? Náhodná slova? Zrada se může schovávat už jen v tom, jak byla otázka položena. Opravdu jsou znaky náhodné, nebo si včelky... vlastně i lidi volí heslo, co si snadno zapamatují?

Ze zkušenosti (a uniklých databází hesel z populárních stránek) víme, že málokdo si navolí bezpečné heslo typu „4zfŭ5d5“, většinou připomíná spíš něco jako „moUrek34“. Ti, co si navolí heslo složitější, velmi často vzdají své pokusy poté, co jsou vyzváni ke změně po každém půl roce (což je také dobrý nápad, heslo může někam uniknout). Pamatovat si takto složitá hesla nezvládnou ani pilné včelky – a to my lidé jsme oproti nim vcelku líní.

Poznámka 1: K tomu, pokud si místo více různých hesel zvolíme jediné heslo, nebo za nás necháme hesla zapamatovat počítač, riskujeme, že jedním únikem přijdeme o všechno.

Někdo může namítnout, že u hesel složených ze slov mohou lidé používat slova velmi častá slova – a tím také usnadní jeho uhádnutí zlým útočníkem (vosou). To je pravda a dobrá připomínka, ale budme k sobě upřímní. Dokážeme se spíše donutit do zapamatování hesla složeného z náhodných slov, nebo náhodných znaků?

Můžeme si vygenerovat s pomocí nástroje několikrát 3 náhodná slova:

- Seminář, Herec, Violoncello
- Duše, Počítač, Slavnost
- Košile, Model, Dluhopis
- Lampa, Algoritmus, Buněk

Porovnejme si to se znaky:

- d8ZaRX5
- KBuGYd3
- XK61wLr
- OH5vzg0

Kterou variantu si spíše zapamatujete? Nehledě na vaše paměťové schopnosti, obojí je podobně náročné pro počítač na uhodnutí, jen v prvním případě musí zkoušet slova a v druhém znaky.

Navíc, spolu s rostoucím výkonem počítačů (podobně jako vosy zvládly po čase díky lepší organizaci rychleji prolamovat medový trezor) se prodlužuje i potřebná bezpečná délka. Je snadnější si zapamatovat o 1 slovo navíc nebo tři další znaky? **Nutno dodat, že už při čtyřech až pěti českých slovech se takto dostáváme na úroveň hesla, která může být bezpečná i dnes**, přestože nejlepší počítače na světě dokážou za sekundu provést operací nikoli stovky jako vosy se svými křídly, ale biliony.

Poznámka 2: Není dobrý nápad se spoléhat na neověřené online nástroje, nemusí být úplně náhodné. Naopak, vzít si do ruky Slovník spisovné češtiny (ten obsahuje více než 250 tisíc slov), otevřít si po sobě několik stránek a se zavřenýma očima ukázat prstem na slova nemusí být špatná cesta.

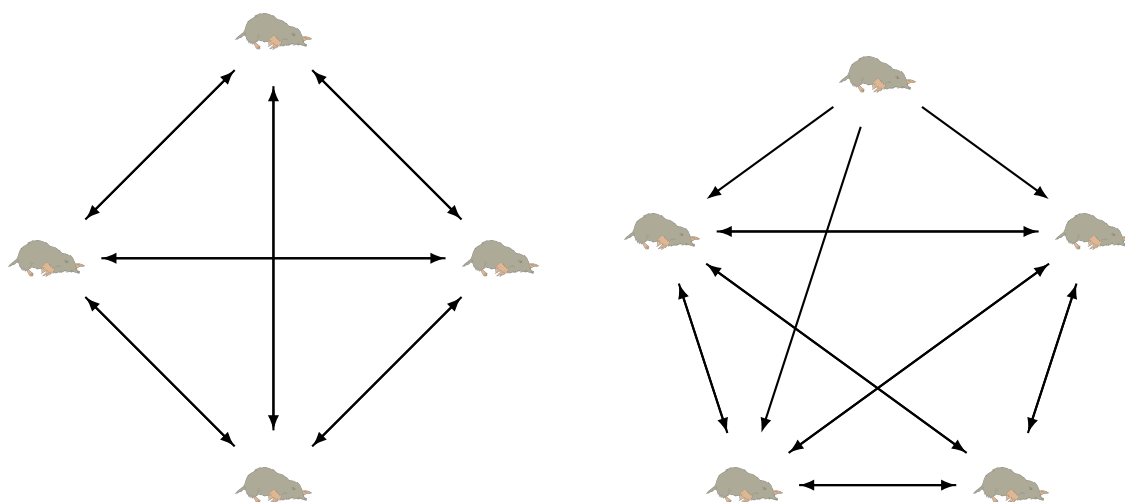
Dovolím si na závěr citovat postarší komiks (<https://xkcd.com/936/>): „Za poslední desítky let snahy jsme úspěšně všechny naučili používat hesla, která jsou pro lidi složitá na zapamatování, ale pro počítač jednoduchá na uhodnutí.“

Kategorie starší

Úloha 1B Ztraceni v davu

Prvně si rozmyslíme, jaká bude nejmenší možná skupina, která bude držet pospolu, pokud každé zvířátko sleduje k různých zvířátek. To bude $k + 1$, právě v takové skupině by mohlo každé zvířátko sledovat všechny ostatní zvířátka v této skupině. Všimněte si, že taková skupina určitě nemůže být menší než $k + 1$, protože každé zvířátko sleduje k jiných zvířátek.

Poradíme prvně výpravě devíti krtků. Kdybychom vybrali $k = 3$, tak by se krtci mohli rozdělit na dvě skupiny (viz obrázek 6). Kdybychom však vybrali $k = 4$, tak nejmenší možná skupina, která bude držet pospolu, bude velká $k + 1 = 5$. Tím pádem se 9 krtků nemůže rozdělit na dvě skupiny, protože by každá skupina musela mít alespoň 5 krtků, tudíž by muselo být celkově 10 krtků, ale krtků je jenom 9. Krtkům tedy poradíme, aby každý sledoval alespoň 4 krtky.



Obrázek 6: rozdělené skupiny krtků pro $k = 3$

Stejný postup použijeme pro celou výpravu, která má 2025 zvířátek. Kdybychom vybrali $k = 1011$, tak by se nám mohla výprava rozdělit na dvě skupiny, jedna s 1012 zvířátky a druhá s 1013 zvířátky. Kdybychom však vybrali $k = 1012$, tak nejmenší možná skupina, která bude držet pospolu, bude velká $k + 1 = 1013$. Tím pádem se 2025 zvířátek nemůže rozdělit na dvě skupiny, protože by každá skupina musela mít alespoň 1013 zvířátek, tudíž by muselo být celkově 2026 zvířátek, ale zvířátek je jenom 2025. Výpravě tedy poradíme, aby každé zvířátko sledovalo alespoň 1012 zvířátek.

Úloha 2B Zrající vinná réva

Nejdůležitější je určit správný počet trsů, které bude Richard sbírat, a jejich pozice, abychom mohli určit, na které trsy dosáhne a na které ne. Víme, že konstrukce měří na výšku 4 m (pro lepší počítání převedeme na 400 cm) a na šířku 6 m (po převedení 600 cm).

Nejprve se zaměříme na trsy, které rostou do výšky. Tím, že všechny trsy rostou 15 cm od okraje, musíme od 400 cm odečíst celkem 30 cm (odečítáme oba okraje). Tímto získáme 370 cm. Vertikálně jsou od sebe trsy vzdálené 74 cm, takže nám stačí 370 cm vydělit 74 cm. Výsledek 5 je počet mezer, jelikož mezery jsou 74 cm. Tím pádem musíme k 5 přičíst ještě 1 a získáme vertikálně 6 trsů vinné révy.

Poté se zaměříme na trsy, které rostou do šířky. Stejně jako předtím odečteme od 600 cm okrajových 30 cm a dále budeme počítat s 570 cm. Horizontálně jsou od sebe vzdálené 38 cm, takže po vydělení nám vyjde 15, což je počet mezer. Pro počet hroznů zase přičteme 1, takže horizontálně máme 16 trsů.

Celkový počet je $6 \cdot 16 = 96$ trsů.

Dále zjistíme pozice trsů, abychom později věděli, za jakých podmínek dosáhne srdečný lev Richard na různé trsy. Můžeme si určit, že levý dolní roh je 0.

Trsy budou v několika úrovních.

Do výšky bude první 15 cm nad zemí a každý další bude o 74 cm výše, takže další rostou v 89 cm, 163 cm, 237 cm, 311 cm a 385 cm.

Do šířky bude první 15 cm od okraje a každý další bude o 38 cm dále, takže další rostou v 53 cm, 91 cm, 129 cm, 167 cm, 205 cm, 243 cm, 281 cm, 319 cm, 357 cm, 395 cm, 433 cm, 471 cm, 509 cm, 547 cm a 585 cm.

Na obrázku 7 jsou tyto úrovně znázorněny světle šedými čarami.



Žebřík má 200 cm a 9 stupíneků. 200 cm musíme vydělit počtem mezer (mezery jsou pro nás i okraje žebříku, což je o 1 více, tedy 10). Takže jedna mezerka je 20 cm, takže první stupínek je 20 cm nad zemí, další 40 cm, 60 cm, 80 cm, 100 cm, 120 cm, 140 cm, 160 cm a 180 cm.

Nejdůležitější je, zjistit, kdy Richard dosáhne na nejvyšší trsy, které jsou v úrovni 385 cm nad zemí. Určitě musí na žebřík, jelikož samotný lev Richard má lopatky 150 cm nad zemí, když natáhne tlapy přímo nahoru, tak dosáhne do výšky 220 cm.

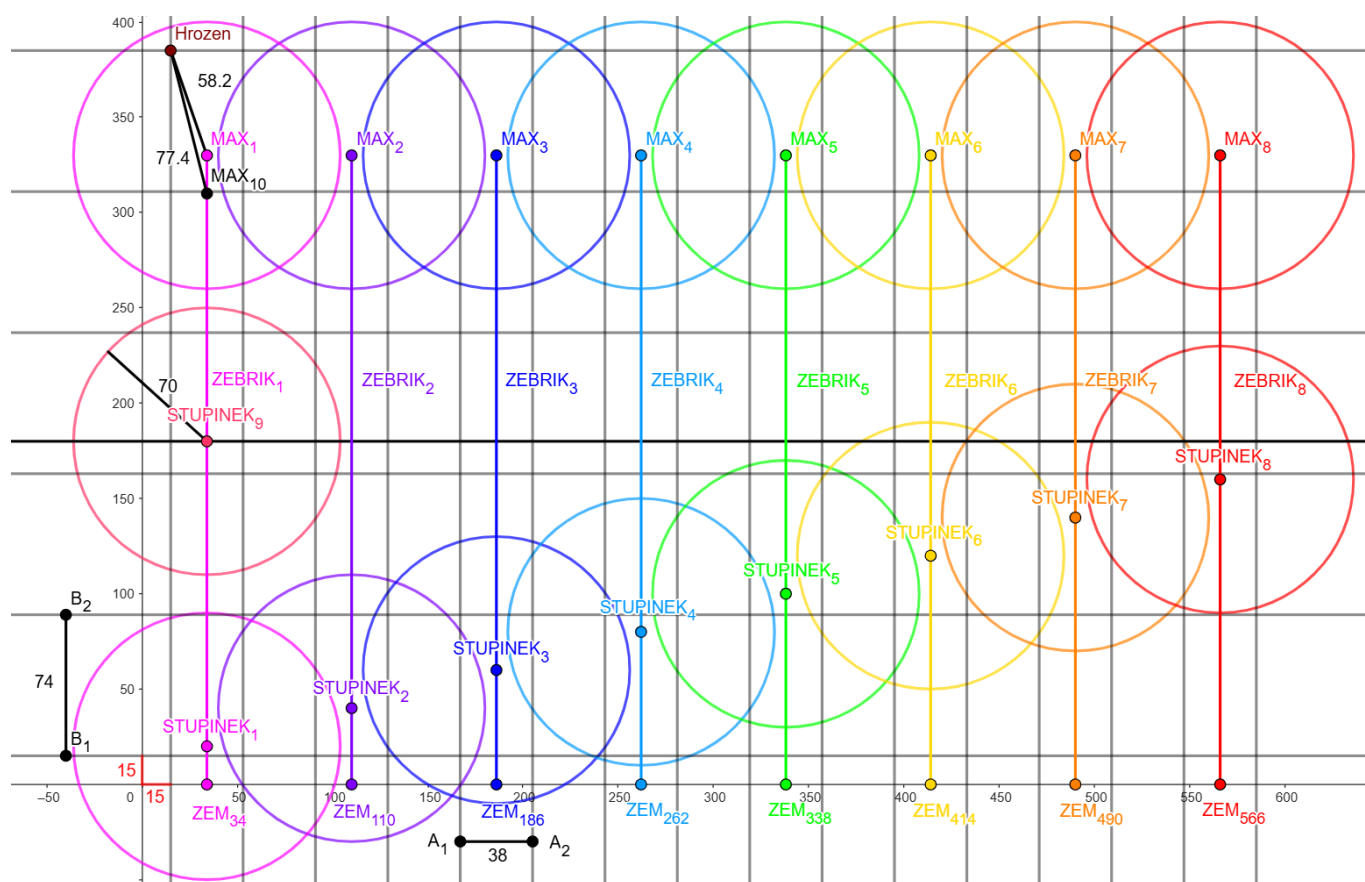
Žebřík staví vždy mezi dva sloupce, takže pokud by postavil první žebřík mezi sloupce vzdálené 15 cm a 53 cm, tak bude střed žebříku postavený v 34 cm (na obrázku 7 je tento žebřík zobrazen růžovou barvou).

Když lev Richard vyleze na 9. stupínek, tak jeho lopatky budou ve výšce $180 \text{ cm} + 150 \text{ cm} = 330 \text{ cm}$. (Na obrázku 7 znázorněno jakožto MAX_1)

Pomocí vzorečku pro výpočet pravoúhlého trojúhelníku vypočítáme, zda lev Richard dosáhne z 9. stupínku na nejvyšší trsy. Musíme určit obě odvěsny. Vodorovná odvěsna se bude rovnat $34 - 15 = 19$. Svislá odvěsna je $385 - 330 = 55$. Dosadíme do vzorečku $c^2 = a^2 + b^2$, takže budeme mít $c^2 = 19^2 + 55^2$, což vyjde po zaokrouhlení na desetiny 58,2, takže určitě dosáhne, jelikož $58,2 < 70$.

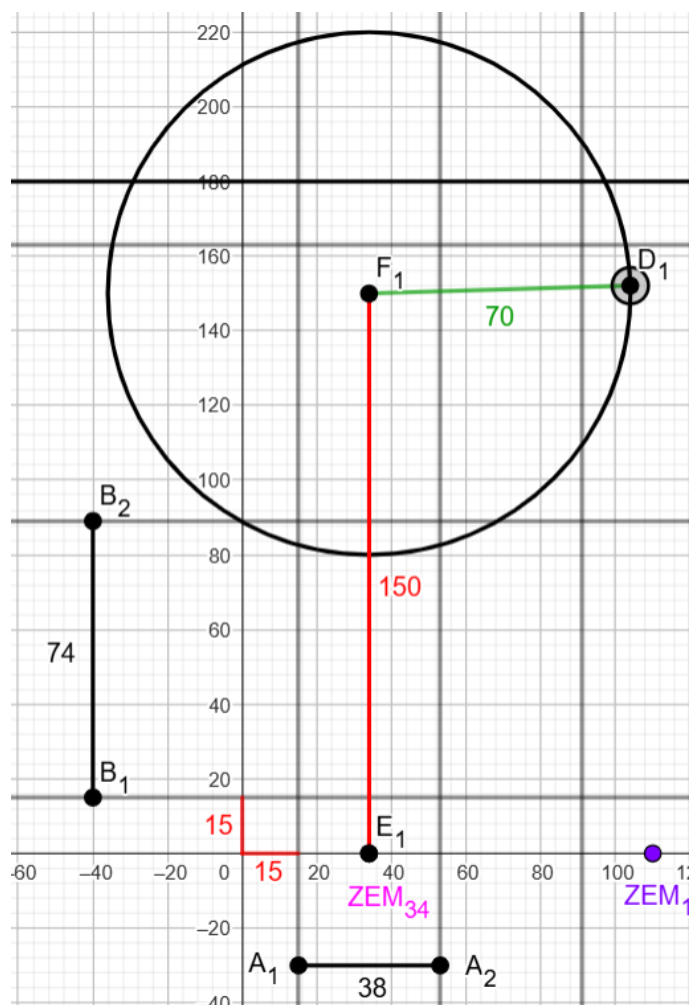
Pro jistotu můžeme vypočítat, zda dosáhne lev Richard na nejvyšší trs i z 8. stupínku. Zase použijeme vzorec pro pravoúhlý trojúhelník. Jedna odvěsna bude opět 19. Pro druhou odvěsnu musíme prvně zjistit výšku lopatek na 8. stupínku, což bude $160 + 150 = 310$ (na obrázku 7 znázorněno jakožto MAX_{10}), čímž odečteme $385 - 310 = 75$. Dosadíme do vzorečku $c^2 = 19^2 + 75^2$, což po zaokrouhlení na desetiny vyjde 77,4, takže z 8. stupínku určitě nedosáhne, jelikož $77,4 > 70$.

Tak jsme ověřili, že Richard musí vylézt až na 9. stupínek, aby dosáhl na nejvyšší trsy. Z obrázku 7 vidíme už bez počítání, že dosáhne vždy na 2 nejvyšší, takže bude muset žebřík pokládat ob jednu mezeru mezi sloupci. Žebřík kvůli tomu bude přesouvat $7 \times$.



Obrázek 7: Náčrty vinné révy a pozice žebříku

Ohledně sbírání víme, že mu stačí vždy sbírat ty trsy, které jsou podél žebříku, jelikož ho musí přesouvat ob mezeru. Na nejvyšší trsy nedosáhne, protože $150 \text{ cm} - 70 \text{ cm} = 80 \text{ cm}$. a nejvyšší trsy jsou 15 cm nad zemí. Pro nejvyšší trsy se musí sehnout. Další trsy jsou 89 cm nad zemí, takže na ty už dosáhne narovnaný.



Obrázek 8: Náskres srdečného lva Richarda

Ted' už nám stačí pouze spočítat kolikrát provede kterou akci, jelikož na pořadí vůči času nezáleží.

Prvotní pozice žebříku bude v tomto případě úplně vlevo a potrvá 3 min = 180 s.

Sebrání trsů a hození do koše trvá celkem 1 s + 1,5 s = 2,5 s, tento čas musíme vynásobit celkovým počtem všech trsů $2,5 \text{ s} \cdot 96 = 240 \text{ s}$. Žebřík zvedne 7× a položí ho 7×, takže $14 \cdot 30 \text{ s} = 420 \text{ s}$. Též přesunutí mu trvá 30 s a přesune ho 7× ob jeden sloupec, takže $30 \text{ s} \cdot 7 = 420 \text{ s}$.

Stupínky musí vylézt i slézt všechny $9 \cdot 2 \cdot 8 \cdot 2 \text{ s} = 288 \text{ s}$. 9 je počet všech stupínků, 2 je proto, že vyleze žebřík nahoru i dolů, 8× vyleze a sleze na žebřík a 2 s je čas, který trvá vylézt nebo slézt jeden stupínek.

Sehnutí trvá 2 s a sehne se celkem 8×, tedy $8 \cdot 2 \text{ s} = 16 \text{ s}$.

Celkový čas sbírání bude $180 \text{ s} + 240 \text{ s} + 420 \text{ s} + 420 \text{ s} + 288 \text{ s} + 16 = 1564 \text{ s}$, převedeme na minuty a zaokrouhlíme na setiny $1564 \text{ s} / 60 = 26,1 \text{ min} = 26 \text{ min } 4 \text{ s}$.

Úloha 3B Med-vědí banka – starší

Podúloha i)

Jediná možná hesla jsou čísla od 0000 po 9999, kterých je přesně 10000 možných (4 číslice po 10 možnostech, celkem tedy $10 \cdot 10 \cdot 10 \cdot 10 = 10000$).

Pokud vosy dokážou každou sekundu zadat přesně 20 hesel, vyzkoušet všechna hesla jim potrvá maximálně $\frac{10000}{20} = 500$ sekund, tedy 8 minut a 20 sekund!

Poznámka bokem, k řešení není potřeba: Často se pro takové číslo používá zkrácený zápis $10 \cdot 10 \cdot 10 \cdot 10 = 10^4$ (deset na čtvrtou), protože násobíme po sobě čtyři desítky a nechce se nám je všechny vypisovat. Je to podobné, jako známe u násobení a sčítání – místo $10 + 10 + 10 + 10$ napíšeme $10 \cdot 4$. Pro čísla začínající na jedničku a pokračující pouze nulami navíc platí hezké pravidlo, že se rovná deseti právě „na tolikátou“, kolik má počet nul, takže $10 = 10^1$, $100 = 10^2$, $1000 = 10^3$ a tak dále.



Podúloha ii)

Pro každý znak hesla nyní existuje 62 možných hodnot (26 malých písmen, 26 velkých písmen a 10 číslic). Protože jednotlivé znaky nemohou ovlivnit jiné, jsou všechny pozice na sobě nezávislé. Celkový počet možných kombinací tak lze dostat tím, že se 62 vynásobí tolikrát, kolik má heslo znaků, nebo-li 62 se umocní na tolikátou, kolik znaků má heslo.

Protože musí existovat alespoň 1 000 000 000 000 (10^{12} , viz poznámka výše) možných hesel, je potřeba zjistit, na kolikátou umocnit základ 62, aby byl výsledek $\geq 1\,000\,000\,000\,000$.

Dopočítat se ke správné délce hesla můžeme tím, že budeme zkoušet pro kolik znaků je heslo dostatečně dlouhé. Jednoduše lze spočítat, že $62 \cdot 62 \cdot 62 \cdot 62 \cdot 62 \cdot 62 = 62^6 \doteq 5,6 \cdot 10\,000\,000\,000$ (přibližně), zatímco $62 \cdot 62 \cdot 62 \cdot 62 \cdot 62 \cdot 62 \cdot 62 = 62^7 \doteq 3,5 \cdot 1\,000\,000\,000\,000$ (přibližně), což již stačí. Takto lze tedy také zjistit, že Vendy si vytvoří nové heslo o délce 7 znaků.

Vosám zabere vyzkoušení všech možných hesel zhruba $3,5 \cdot 10\,000\,000\,000$ sekund, což je asi 1100 let. Vendy už může doufat, že je její heslo v bezpečí.

(Poznámka bokem: Pokud je někdo opravdu hodně vepředu s učivem a zná funkci zvanou logaritmus, může si spočítat, že $\log_{62} 10^{12} \doteq 6,7$ a je tedy potřeba alespoň 7 znaků dlouhé heslo. Tím se ale teď nemusíte trápit, logaritmy vás čekají až na střední škole a nikdo je po vás nebude chtít v tuto chvíli ani na Matematické olympiádě.)

Podúloha iii)

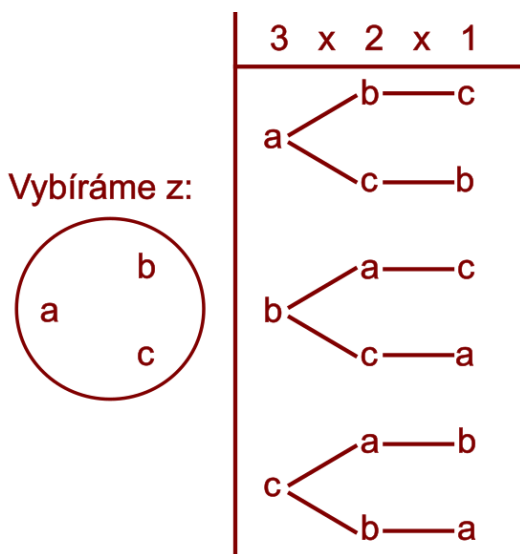
Vendy ví, ze kterých 7 znaků se heslo skládá, ale neví jejich pořadí. Pořadí 7 různých věcí lze spočítat tak, že na první pozici může být libovolný znak ze znaků, co si pamatuje. Na druhé už ale vybírá pouze z 6 možných znaků, protože první už si vybrala, ať už byl jakýkoli. Tím má vlastně vypsané všechny možné kombinace prvních dvou znaků hesla.

Na třetí jí tedy zbývá pokaždé už jen 5 zbylých možných znaků a takhle postupně získá všechna možná seřazení znaků (až na poslední pozici může být jen jeden přesně daný znak).

Celkový počet možných vyhovujících hesel tak je $7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5040$. Při variantě s 8 znaky je přesně 5040 způsobů, jak uspořádat posledních 7 znaků a 8 způsobů, jak vybrat první znak, celkem tedy $8 \cdot 5040 = 40320$.

Ostatně, že to funguje si můžete vyzkoušet sami na menším hesle:

- Napište si na papír pod sebe nejdříve třeba tři různé znaky **a**, **b**, **c**.
- Poté si za ně запиšte, jaké všechny znaky mohou být na první pozici: inu, buď **a**, nebo **b**, nebo **c**.
- Pokud už jste na začátku zvolili **a**, vedou z něj už jen dvě možnosti na to, jaký znak může být na druhé pozici – buď **b**, nebo **c** (a už máme na první). Obdobně pro druhou pozici u možných hesel začínajících na **b** nebo **c**.
- Na třetí a poslední pozici už nám vždycky zbude jen jeden znak, protože jsme pokaždé vybrali dva ze tří možných znaků z naší pomyslné hromádky.
- Možných hesel je tedy $3 \cdot 2 \cdot 1$.



Obrázek 9: Pořadí znaků hesla názorně

Podúloha iv)

Zde se počet možností bude počítat stejně jako v části ii), akorát místo s číslem 62 je potřeba počítat s číslem 314 159.

Budeme opět postupně násobit počet možností, jen ne pro jeden znak samostatně, ale pro počet slov (což je v našem případě 314 159). Pro dvě slova lze zjistit, že kombinací je $314\,159 \cdot 314\,159 = 314\,159^2 \doteq 9,9 \cdot 10\,000\,000\,000$, zatímco $314\,159 \cdot 314\,159 \cdot 314\,159 = 314\,159^3 \doteq 3,1 \cdot 10\,000\,000\,000\,000$. Takto lze také zjistit, že stačí tři slova.

Pro představu, pokud by vosy zkoušely všechny kombinace tří slov rychlostí 20 hesel za sekundu, trvalo by jim to necelých 50 000 000 let.

(Možným řešením pro silně pokročilé je i zde spočítat $\log_{314159} 10^{12} \doteq 2,2$, potřeba jsou tedy jen tři slova.)

Podúloha v)

Pro každé pětispísmenné slovo jsou úpravy na něm možné stejné, stačí tedy spočítat, kolik možných úprav lze učinit na jednom takovém slově a vynásobit tento počet počtem pětiznakových slov (15 427).

V každém slově je právě jedno písmeno velké, je tedy jen 5 možností, které to může být. Dále je jedno další písmeno nahrazeno číslicí, to je celkem $10 \cdot 4$ (Písmeno, které je velké, nelze nahradit číslicí). Navíc je na konci každého slova jedna další číslice, to je dalších 10 možností. Jedno slovo tedy lze upravit jen $5 \cdot 4 \cdot 10 \cdot 10 = 2\,000$ způsoby.

Celkový možný počet takovýchto hesel je pak $15\,427 \cdot 2\,000 = 30\,854\,000$. Vosy toto heslo vyzkouší nejpozději po 308 540 sekundách, což je asi 86 hodin.

Podúloha vi)

V této úloze dostali bod prakticky všichni, kdo zkusili zauvažovat nad tím, jaké heslo by mohlo být bezpečnější a proč.

Jaká možnost je ale nakonec lepší? Náhodné znaky? Náhodná slova? Zrada se může schovávat už jen v tom, jak byla otázka položena. Opravdu jsou znaky náhodné, nebo si včelky... vlastně i lidi volí heslo, co si snadno zapamatují?

Ze zkušenosti (a uniklých databází hesel z populárních stránek) víme, že málokdo si navolí bezpečné heslo typu „4zfũ5d5“, většinou připomíná spíš něco jako „moUrek34“. Ti, co si navolí heslo složitější, velmi často vzdají své pokusy poté, co jsou vyzváni ke změně po každém půl roce (což je také dobrý nápad, heslo může někam uniknout). Památovat si takto složitá hesla nezvládnou ani pilné včelky – a to my lidé jsme oproti nim vcelku líní.

Poznámka 1: K tomu, pokud si místo více různých hesel zvolíme jediné heslo, nebo za nás necháme hesla zapamatovat počítač, riskujeme, že jedním únikem přijdeme o všechno.

Někdo může namítnout, že u hesel složených ze slov mohou lidé používat slova velmi častá slova – a tím také usnadní jeho uhádnutí zlým útočníkem (vosou). To je pravda a dobrá připomínka, ale budme k sobě upřímní. Dokážeme se spíše donutit do zapamatování hesla složeného z náhodných slov, nebo náhodných znaků?

Můžeme si vygenerovat s pomocí nástroje několikrát 3 náhodná slova:

- Seminář, Herec, Violoncello
- Duše, Počítač, Slavnost
- Košile, Model, Dluhopis
- Lampa, Algoritmus, Buněk

Porovnejme si to se znaky:

- d8ZaRX5
- KBuGYd3
- XK61wLr
- OH5vzg0

Kterou variantu si spíše zapamatujete? Nehledě na vaše paměťové schopnosti, obojí je podobně náročné pro počítač na uhodnutí, jen v prvním případě musí zkoušet slova a v druhém znaky.

Navíc, spolu s rostoucím výkonem počítačů (podobně jako vosy zvládly po čase díky lepší organizaci rychleji prolamovat medový trezor) se prodlužuje i potřebná bezpečná délka. Je snadnější si zapamatovat o 1 slovo navíc nebo tři další znaky? **Nutno dodat, že už při čtyřech až pěti českých slovech se takto dostáváme na úroveň hesla, která může být bezpečná i dnes**, přestože nejlepší počítače na světě dokážou za sekundu provést operací nikoli stovky jako vosy se svými křídly, ale biliony.

Poznámka 2: Není dobrý nápad se spoléhat na neověřené online nástroje, nemusí být úplně náhodné. Naopak, vzít si do ruky Slovník spisovné češtiny (ten obsahuje více než 250 tisíc slov), otevřít si po sobě několik stránek a se zavřenýma očima ukázat prstem na slova nemusí být špatná cesta.

Dovolím si na závěr citovat postarší komiks (<https://xkcd.com/936/>): „Za poslední desítky let snahy jsme úspěšně všechny naučili používat hesla, která jsou pro lidi složitá na zapamatování, ale pro počítač jednoduchá na uhodnutí.“