Paní uklízečka a svazek neoznačených klíčů

Paní uklízečka jde poprvé do služby. Má uklidit v N místnostech, dostane N různých klíčů, které k místnostem patří, ale klíče nejsou označené. Jaký je nejpravděpodobnější počet pokusů, na který otevře všechny dveře?

Předpokládáme přitom, že uklízečka si všechny předchozí pokusy pamatuje a že postupuje nejefektivněji jak je jen možné. „Pokusem“ se myslí každé zastrčení klíče do zámku.

Řešení:

V rámci řešení nejenom najdeme onen nejpravděpodobnější počet pokusů, ale rovnou určíme celou pravděpodobnostní funkci (rozdělení pravděpodobnosti). Jediným parametrem úlohy je počet dveří N.

Strategie Bez újmy na obecnosti můžeme definovat algoritmus, podle něhož bude postupovat; žádný „efektivnější“ neexistuje:
Uklízečka půjde k prvním dveřím a bude postupně zkoušet všechny klíče, dokud nenarazí na ten správný. Označíme jej (stejně jako ona) `1`. Potom jde ke druhým dveřím a zkouší všechny kromě `1`, jakmile narazí na správný, označí si jej `2` atd. U předposledních dveří zkouší už jen dva klíče a poslední dveře pochopitelně otevírá najistotu klíčem s označením `N`.

Definice a značení *Posloupností pokusů* máme na mysli chronologicky seřazený záznam všech pokusů vedoucí k otevření všech dveří, přičemž podtržené číslo značí úspěšný pokus: např. $\texttt{24}\underline{\texttt{1}}\texttt{4}\underline{\texttt{234}}$ pro $N = 4$. Počet všech pokusů budeme nazývat *délkou posloupnosti*; uvedený příklad má délku 7.

Posloupnosti (v našem případě to budou konkrétně pravděpodobnostní funkce diskrétních rozdělení) budeme indexovat hranatými závorkami, tj. třeba $x[n]$. Posloupnost, která nabývá jedničky pouze pro indexy u až v, jinde nabývá nuly, budeme značit $\mathrm{rec}(\{u, \ldots, v\})$.

Nejkratší a nejdelší posloupnosti Nejkratší posloupnost odpovídá případu, že všechny dveře otevře na první pokus, celkem je to $d_{\min} := N$ pokusů. Nejdelší naopak případu, kdy každé z dveří otevře až na pokus poslední, zbývající. Pokusů v tomto případě je $N + (N - 1) + (N - 2) + \ldots + 2 + 1$, což je součet aritmetické posloupnosti s výsledkem $d_{\max} := \frac{N^2+N}{2}$. Pro dané N je tedy celkem $d_{\max} - d_{\min} + 1 = \frac{N(N-1)}{2} + 1$ možných délek posloupností pokusů.

Příklad Pro $N = 3$ dveře jsou možnosti následující: Existuje pouze jedna varianta s délkou posloupnosti 3 (posloupnost pokusů $\underline{123}$). Čtyři pokusy lze dosáhnout třemi variantami ($\underline{1}3\underline{23}$, $3\underline{123}$, $2\underline{123}$). Pro pět pokusů existují čtyři varianty ($23\underline{123}$, $2\underline{1}3\underline{23}$, $32\underline{123}$, $3\underline{1}3\underline{23}$) a šest pokusů je možné dosáhnout pouze dvěma variantami ($32\underline{1}3\underline{23}$, $23\underline{1}3\underline{23}$). Další možnosti neexistují.

Jaká je pravděpodobnost, že nastane některá z posloupností určité délky? Vezměme např. posloupnost $\underline{1}3\underline{23}$. Pravděpodobnost, že nastane tento případ, je roven $\frac{1}{3} \cdot \frac{1}{2} \cdot 1 \cdot 1 = \frac{1}{6}$. Vezměme posloupnost stejné délky $3\underline{123}$. Její pravděpodobnost je $\frac{1}{3} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot 1 = \frac{1}{12}$ a stejně tak je tomu s posloupností $2\underline{123}$. Celkově tedy na čtyři pokusy se podaří otevřít všechny dveře s pravděpodobností $\frac{1}{6} + \frac{1}{12} + \frac{1}{12} = \frac{1}{3}$.

Každá z variant posloupností délky 5 má shodnou pravděpodobnost, a to $\frac{1}{12}$. Tedy pravděpodobnost, že celkový počet pokusů bude 5, je $4 \cdot \frac{1}{12} = \frac{1}{3}$.

Délka posloupnosti	3	4	5	6
Počet variant	1	3	4	2
Pravděpodobnost této délky	$\frac{1}{6}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{6}$

Tabulka shrnuje fakta pro $N = 3$. Je vidět, že počet variant nemusí korespondovat s výslednou pravděpodobností. Zároveň je patrné, že maximum (což hledáme) se vyskytuje na dvou místech současně.

Situace u jedněch dveří Pokud přijmeme výše uvedenou strategii, pak u každých dveří se snažíme najít ten správný z K klíčů (přičemž postupně $K = N$ až $K = 1$).

Lemma 1: Nechť X_K je náhodná veličina představující počet pokusů u K-tých dveří až do nalezení správného klíče (včetně). To znamená, že X_K může nabýt hodnoty $k = 1, \dots, K$. Potom $P(X_K = k) = \frac{1}{K}$ a tedy na k nezávisí, všechny počty pokusů jsou tudíž shodně pravděpodobné.

Důkaz. Platí $P(X_K = k) = \frac{K-1}{K} \cdot \frac{K-2}{K-1} \cdot \ldots \cdot \frac{K-k+1}{K-k+2} \cdot \frac{1}{K-k+1} = \frac{1}{K}$. $\square$

Tedy díky tomu lze X_K považovat za náhodnou veličinu s rovnoměrným rozdělením pravděpodobnosti, $X_K \sim \mathrm{Ud}(\{1, \dots, K\})$. Označme jí příslušnou pravděpodobnostní funkci symbolem p_K, přičemž zřejmě

$$p_K[n] = \begin{cases} \frac{1}{K} & \text{pro } n = 1, \dots, K, \\ 0 & \text{jinde.} \end{cases}$$

To znamená, že můžeme psát $p_K[n] = \frac{1}{K}\mathrm{rec}(\{1, \dots, K\})$.

Celková situace Celkový počet pokusů pro N dveří je náhodná veličina $X(N) = X_N + X_{N-1} + \ldots + X_1$, což znamená

$$X(N) \sim \sum_{i=1}^{N} \mathrm{Ud}(\{1, \ldots, i\}). \tag{1}$$

Úkolem úlohy je tedy vlastně najít maximum pravděpodobnostní funkce $X(N)$. Přitom je zřejmé, že počet pokusů u jedněch dveří není ovlivněn počtem pokusů u jiných, takže jsou to nezávislé náhodné veličiny.

Pravděpodobnostní funkce Odvoďme pravděpodobnostní funkci pro (1).

Lemma 2*:* Nechť F a G jsou nezávislé náhodné veličiny s diskrétním rozdělením pravděpodobnosti, tak že jejich pravděpodobnostní funkce je definovaná v celočíselných hodnotách. Pokud $f[n]$ je pravděpodobnostní funkcí veličiny F a $g[n]$ je pravděpodobnostní funkcí G, pak součet náhodných veličin $H = F + G$ má pravděpodobnostní funkci danou konvolucí jejich pravděpodobnostních funkcí, $h[n] = f[n] * g[n]$.

Důkaz. Jestliže H má nabýt zvolené fixní hodnoty řekněme $m \in \mathbb{Z}$, pak toho je dosaženo právě tak, že pokud F nabyde hodnoty r a G hodnoty $m - r$, a to pro jakékoliv $r \in \mathbb{Z}$. Můžeme tedy napsat, že $P(H = m) = \sum_{r=-\infty}^{\infty} P(F = r) \cdot P(G = m - r)$. Protože m je libovolné celé číslo, můžeme napsat ekvivalentně $h[n] = \sum_{r=-\infty}^{\infty} f[r]g[m - r]$, což je definice konvoluce. □

Protože náhodná veličina (1), o jejíž rozložení se zajímáme, je dána součtem náhodných veličin, které splňují předpoklady uvedeného tvrzení, pravděpodobnostní funkce pro $X(N)$ je konvolucí jednotlivých pravděpodobnostních funkcí:

$$p(N) := p_N[n] * p_{N-1}[n] * \ldots * p_2[n] * p_1[n]. \tag{2}$$

neboli rekurzivně: $p(N) = p_N[n] * p(N - 1)$ pro $N \geq 2$, když $p(1)$ definujeme jako jedničku v jedničce.

Intermezzo Značením $\mathbb{Z}+\frac{1}{2}$ budeme myslet množinu $\{\ldots, -\frac{3}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \ldots\}$. Řekneme, že posloupnost $f[n]$ je symetrická okolo $a \in \mathbb{Z}$, resp. $a \in \mathbb{Z} + \frac{1}{2}$ (*a-sudost*), pokud platí $f[a - n] = f[a + n]$ pro všechna $n \in \mathbb{Z}$, resp. $a \in \mathbb{Z} + \frac{1}{2}$. (Definice koresponduje s pojmy *whole-point symmetry*, resp. *half-point symmetry* používanými v literatuře).

Hledání maxima Intuice a simulace (viz dále) napovídají, že maximální pravděpodobnost nastane „vprostřed" intervalu možných hodnot (tedy $d_{\min} = N$ a $d_{\max} = \frac{N^2+N}{2}$). Uvedeme kroky (bez důkazů), které nás k tomu dovedou.

Lemma 3*:* Je-li $f[n]$ je symetrická okolo a a $g[n]$ je symetrická okolo b, pak jejich konvoluce $f[n] * g[n]$ je sudá okolo $a + b$.

Lemma 4*:* Je-li $f[n]$ nezáporná, symetrická okolo a, rostoucí až do a (tj. $f[n - 1] < f[n]$ pro $n \leq a$), s kompaktním nosičem, a $g[n]$ je konstantní kladná s kompaktním nosičem (a tedy je také symetrická, řekněme okolo b), pak konvoluce $f[n]*g[n]$ je nezáporná, s kompaktním nosičem, symetrická okolo $a+b$, rostoucí do $a + b$.

Důsledek 5*:* Za předpokladu právě uvedeného tvrzení má konvoluce $f[n] * g[n]$ buď jediné maximum v indexu $a + b$ nebo dvě maxima v indexech $a + b - \frac{1}{2}$ a $a + b + \frac{1}{2}$.

Lemma 6*:* Nachází-li se nosič $f[n]$ mezi indexy r_f a s_f, a nosič $g[n]$ mezi r_g a s_g, pak $f[n] * g[n]$ má nosič $\{r_f + r_g, \ldots, s_f + s_g\}$.

Vztah (2) říká, že výsledná pravděpodobnostní funkce je mnohonásobnou konvolucí konstantních posloupností, což lze napsat

$$
\begin{aligned}
p(N) &:= \frac{1}{N}\mathrm{rec}(\{1, \ldots, N\}) * \ldots * \frac{1}{2}\mathrm{rec}(\{1, 2\}) * \frac{1}{1}\mathrm{rec}(\{1\}) \qquad (3)\\
&= \frac{1}{N!} \cdot \mathrm{rec}(\{1, \ldots, N\}) * \ldots * \mathrm{rec}(\{1, 2\}) * \mathrm{rec}(\{1\}). \qquad (4)
\end{aligned}
$$

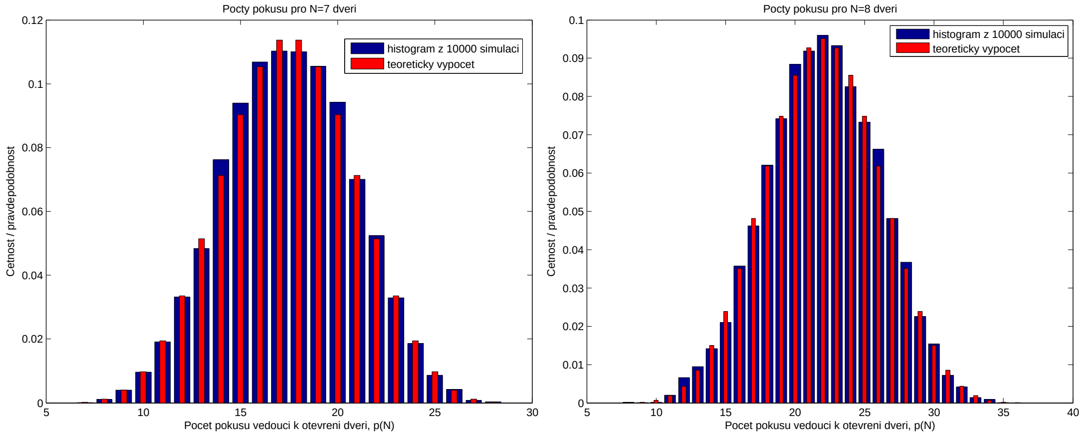
Postupujme v (4) zprava: první konvoluce (je to vlastně $p(2)$ až na konstantu) je rovna $\{1, 1\} * \{1\} = \{1, 1\}$, a to na indexech 2 až 3 dle lemmatu 6. Pak další je rovna (koresponduje s $p(3)$) $\{1, 1, 1\} * \{1, 1\} = \{1, 2, 2, 1\}$ na indexech 3 až 6. A tak dále. Nyní využijeme pomocných tvrzení a indukcí dokážeme chtěné.

Tvrzení 7*:* Posloupnost $p(N)$ má jediné maximum, a to v polovině svého nosiče, případně má dvě maxima vzdálená o $\frac{1}{2}$ od středu svého nosiče. Přitom střed nosiče se nachází v čísle $\frac{N(N+3)}{4}$.

Důkaz. Pro $N = 3$ bylo ukázáno explicitně výše, že maxima jsou tam, kde byla očekávána (střed nosiče byl 2,5 pro $N = 2$ a 4,5 pro $N = 3$). Předpokládejme platnost tvrzení pro $N - 1$. Potom $f[n] = p(N - 1)$ a $g[n] = \mathrm{rec}(\{1, \ldots, N\})$ splňují předpoklady výše uvedených tvrzení a tedy pro $p(N)$ platí tvrzení. Výsledný nosič $p(N)$ začíná s ohledem na lemma 6 na indexu $1 + \ldots + 1 = N$ a končí na indexu $1 + 2 + \ldots + N = \frac{N^2+N}{2}$. Střed nosiče je tedy průměr těchto hodnot a to je $\frac{N(N+3)}{4}$. □

Jedno nebo dvě maxima Abychom rozhodli tuto otázku, stačí určit, kdy je $\frac{N(N+3)}{4}$ celé číslo. V takovém případě existuje jediné maximum, jinak máme maxima dvě, díky dříve dokázané symetrii konvoluce.

Lemma 8*:* Číslo $\frac{N(N+3)}{4}$ je celé pro $N = 4, 5, 8, 9, 12, 13, \ldots$ a necelé pro $N = 2, 3, 6, 7, 10, 11, \ldots$



Obrázek 1: Teoretický výpočet versus výsledky simulace pro 10 000 opakování pro $N = 7$ a $N = 8$.

Simulace a ověření teorie Na obr. 1 je vidět soulad teoretického odvození se simulací. V případě $N = 7$ je maximální pravděpodobnost pro 17 a 18 pokusů, pro $N = 8$ je maximum pro počet pokusů 22. Software pro Matlab je možné nalézt na stránce `.../~rajmic/koutek/uklizecka-software`. Je zde vystaven i kód pro Haskell, který generuje úplně všechny možnosti posloupnosti klíčů pro zadané N (děkuji R. Hrbáčkovi).

Závěr a možná nová zadání Ukázali jsme, že nejpravděpodobnější počet pokusů se nachází „vprostřed“ všech možností. Celočíselnost tohoto středu určuje, zda maximum obsazuje pouze jediná možnost a nebo jsou maxima dvě.

Nabízí se otázka, jak by to dopadlo, kdyby se přidala alespoň jedna nekonečná posloupnost? Např. by se přidalo pravidlo, že když uklízečka neotevře všechny dveře do $m \leq m_{\max}$ pokusů, ztratí trpělivost, naštve se, praští klíčema o zem, tím ztratí jejich uspořádání … a po zklidnění musí začít znovu…

Nebo: jak by vypadalo rozdělení počtu pokusů při hraní Pexesa jednoho hráče? Předpokládejme, že hráč by si všechny předchozí své pokusy pamatoval. Jaký je nejpravděpodobnější počet kol, než otočí všech N dvojic kartiček?