

Stirlingova formule

Odvodíme Stirlingovu formuli

$$\log n! \doteq n \log n - n + \frac{1}{2} \log n + \log \sqrt{2\pi}$$

kde $\log$ je the přirozený logaritmus. Znak $\doteq$ zde znamená, že

$$\lim_{n \rightarrow \infty} \log n! - (n \log n - n + \frac{1}{2} \log n + \log \sqrt{2\pi}) = 0.$$

Uvažujme integrál

$$\int_1^n \log x \, dx.$$

Integrujeme per partes ($u' = 1$ a $v = \log x$) a dostaneme

$$\int_1^n \log x \, dx = [x \log x]_1^n - \int_1^n 1 \, dx = n \log n - n + 1$$

a při použití lichoběžníkové metody s krokem rovným 1 dostaneme

$$\int_1^n \log x \, dx = \sum_{k=1}^n \log k - \frac{1}{2} \log n + \delta_n = \log n! - \frac{1}{2} \log n + \delta_n$$

kde δ_n je chyba, která je omezená. Srovnáním těchto dvou výsledků máme

$$\log n! = n \log n - n + \frac{1}{2} \log n + \Delta_n$$

kde $\Delta_n = 1 - \delta_n$. Následující tabulka ukazuje chybu Δ_n pro různé hodnoty n

n	Δ_n
10	0.927269
100	0.919772
1000	0.919022

Ukážeme, že

$$\lim_{n \rightarrow \infty} \Delta_n = \log \sqrt{2\pi} \doteq 0.918939.$$

Za tím účelem budeme uvažovat integrál

$$I_n = \int_0^{\pi} \sin^n x \, dx.$$

Lze snadno spočítat

$$I_0 = \pi,$$

$$I_1 = 2,$$

$$I_2 = \frac{1}{2}\pi.$$

Když integrujeme per partes ($u' = \sin x$ a $v = \sin^n x$), tak dostaneme

$$\begin{aligned} I_{n+1} &= \int_0^{\pi} \sin x \sin^n x \, dx = [-\cos x \sin^n x]_0^{\pi} + n \int_0^{\pi} \cos^2 x \sin^{n-1} x \, dx = \\ &= n \int_0^{\pi} (1 - \sin^2 x) \sin^{n-1} x \, dx = n(I_{n-1} - I_{n+1}). \end{aligned}$$

To dá

$$(1+n)I_{n+1} = nI_{n-1}$$

a

$$I_{n+1} = \frac{n}{n+1} I_{n-1}.$$

Tedy, když začneme s $I_0 = \pi$, tak dostaneme I_n pro sudé n

$$I_0 = \pi$$

$$I_2 = \frac{1}{2}\pi$$

$$I_4 = \frac{3}{4} \frac{1}{2} \pi$$

$$I_6 = \frac{5}{6} \frac{3}{4} \frac{1}{2} \pi$$

$$I_8 = \frac{7}{8} \frac{5}{6} \frac{3}{4} \frac{1}{2} \pi$$

atd. a podobně, když začneme s $I_1 = 2$, tak dostaneme I_n pro liché n

$$I_1 = 2$$

$$I_3 = \frac{2}{3}2$$

$$I_5 = \frac{4}{5}\frac{2}{3}2$$

$$I_7 = \frac{6}{7}\frac{4}{5}\frac{2}{3}2$$

$$I_9 = \frac{8}{9}\frac{6}{7}\frac{4}{5}\frac{2}{3}2$$

atd.

Nyní ukážeme, že

$$\lim_{n \rightarrow \infty} \frac{I_n}{I_{n-1}} = 1.$$

Pro $0 < x < \frac{1}{2}\pi$ a pro $\frac{1}{2}\pi < x < \pi$ máme $0 < \sin x < 1$ a tudíž posloupnost $\sin^n x$ je kladná a klesající s n , takže

$$0 < I_{n+1} < I_n < I_{n-1}.$$

Když vydělíme číslem I_{n-1} , tak dostaneme

$$\frac{n}{n+1} < \frac{I_n}{I_{n-1}} < 1$$

a z věty o dvou policajtech (anglicky the squeeze theorem) dostaneme

$$\lim_{n \rightarrow \infty} \frac{I_n}{I_{n-1}} = 1.$$

Když vyjádříme I_n a I_{n-1} pomocí I_0 a I_1 (zde lze bez újmy na obecnosti uvažovat sudé n), tak dostaneme

$$\lim_{n \rightarrow \infty} \frac{\frac{1 \cdot 3 \cdot 5 \cdots n-1}{2 \cdot 4 \cdot 6 \cdots n} \pi}{\frac{2 \cdot 4 \cdot 6 \cdots n}{1 \cdot 3 \cdot 5 \cdots n+1} 2} = 1.$$

Zde součin lichých čísel můžeme vynásobit sudými čísly, abychom dostali faktorial a podobně součin suchých čísel můžeme vydělit vhodnou mocninou dvou, abychom dostali faktorial. To dá

$$\lim_{n \rightarrow \infty} \frac{\frac{n!}{(2(\frac{n}{2})\frac{n}{2}!)^2} \pi}{\frac{(2(\frac{n}{2})\frac{n}{2}!)^2}{(n+1)!} 2} = 1$$

a po zjednodušení

$$\lim_{n \rightarrow \infty} \frac{n!(n+1)!}{2^{2n} \left(\frac{n!}{2}\right)^4} \frac{\pi}{2} = 1$$

a po odmocnění

$$\lim_{n \rightarrow \infty} \frac{\sqrt{n+1}}{2^n \left(\frac{n!}{2}\right)^2} \sqrt{\frac{\pi}{2}} = 1$$

a logaritmování a s použitím výše odvozeného vztahu

$$\log n! = n \log n - n + \frac{1}{2} \log n + \Delta_n$$

dostaneme

$$\begin{aligned} & \lim_{n \rightarrow \infty} \frac{1}{2} \log(n+1) + n \log n - n + \frac{1}{2} \log n + \Delta_n - \\ & - n \log 2 - 2 \left(\frac{n}{2} \log \frac{n}{2} - \frac{n}{2} + \frac{1}{2} \log \frac{n}{2} + \Delta_{\frac{n}{2}} \right) + \frac{1}{2} \log \frac{\pi}{2} = 0 \end{aligned}$$

a po zjednodušení máme výsledek

$$\lim_{n \rightarrow \infty} \Delta_n = \log \sqrt{2\pi} \doteq 0.918939.$$

Tím je odvozena Stirlingova formule

$$\log n! \doteq n \log n - n + \frac{1}{2} \log n + \log \sqrt{2\pi}.$$

Následující tabulka ukazuje dobrou shodu této aproximace pro různé hodnoty n

n	$\log n!$	$n \log n - n + \frac{1}{2} \log n + \log \sqrt{2\pi}$
10	15.1044	15.0961
100	363.739	363.739
1000	5912.13	5912.13

1 Aplikace

Uvažujme následující úlohu. Jaká je pravděpodobnost, že mezi 22 fotbalisty mají alespoň dva hráči narozeniny stejný den v roce. Nebo obráceně, jaká je pravděpodobnost, že nedojde k souběhu narozenin mezi 22 hráči?

Obecněji, uvažujme množinu $\mathcal{A}$ s k prvky (hráči) a množinu $\mathcal{B}$ s n prvky (dny v roce). Jaká je pravděpodobnost, že náhodně zvolené zobrazení z množiny $\mathcal{A}$ do množiny $\mathcal{B}$ je prosté, tedy pro různé vzory máme různé obrazy?

Pro $k > n$ je pravděpodobnost nesouběhu nulová. Existují alespoň dva různé prvky, které se zobrazí na stejný prvek.

Je-li $k \leq n$, pak, aby nedošlo k souběhu, první prvek z množiny $\mathcal{A}$ se může zobrazit na jakýkoliv z n prvků množiny $\mathcal{B}$. Druhý prvek se může zobrazit na jakýkoliv z $n - 1$ zbývajících prvků množiny $\mathcal{B}$. Třetí prvek množiny $\mathcal{A}$ se může zobrazit na jakýkoliv z $n - 2$ prvků množiny $\mathcal{B}$. Celkový počet zobrazení je n^k . Takže pravděpodobnost nesouběhu je

$$P = \frac{n(n-1)(n-2)(n-3) \cdots (n-k+1)}{n^k} = \frac{n!}{(n-k)! n^k}$$

Pro $k = 22$ a $n = 365$ máme $P = \frac{365!}{(365-22)! 365^{22}} \doteq 0.524305$. Takže pravděpodobnost nesouběhu je přibližně 52 %, tedy pravděpodobnost, že alespoň dva hráči budou mít narozeniny stejný den v roce je přibližně 48 %.

Pro velké n můžeme použít Stirlingovu formuli pro faktorial

$$\log n! \doteq n \log n - n + \frac{1}{2} \log n + \log \sqrt{2\pi}.$$

Pak přirozený logaritmus pravděpodobnosti nesouběhu je

$$\begin{aligned} \log P &= \log \frac{n!}{(n-k)! n^k} \doteq \\ &\doteq n \log n - n + \frac{1}{2} \log n + \log \sqrt{2\pi} - (n-k) \log(n-k) + n-k - \frac{1}{2} \log(n-k) - \log \sqrt{2\pi} - k \log n = \\ &= n \log n + \frac{1}{2} \log n - n \log(n-k) + k \log(n-k) - k - \frac{1}{2} \log(n-k) - k \log n = \\ &= n \log \frac{n}{n-k} + \frac{1}{2} \log \frac{n}{n-k} - k \log \frac{n}{n-k} - k = \\ &= (n-k + \frac{1}{2}) \log \frac{n}{n-k} - k = \\ &= -(n-k + \frac{1}{2}) \log \frac{n-k}{n} - k = \\ &= -(n-k + \frac{1}{2}) \log(1 - \frac{k}{n}) - k. \end{aligned}$$

Nyní rozvineme logaritmus

$$\log(1+x) = x - \frac{1}{2}x^2 + \text{h.o.t.}$$

pro $x = -\frac{k}{n}$, kde h.o.t. značí členy vyšších řádů (anglicky higher order terms).
To nám dá

$$\begin{aligned}\log P &= -(n - k + \frac{1}{2})(-\frac{k}{n} - \frac{1}{2}\frac{k^2}{n^2}) - k + \text{h.o.t.} = \\ &= -\frac{1}{2}\frac{k^2}{n} + \text{h.o.t.}\end{aligned}$$

Můžeme použít tuto aproximaci na výše uvedený příklad s 22 hráči

$$P \doteq \exp(-\frac{1}{2}\frac{22^2}{365}) \doteq 0.515296,$$

což je v souladu s naším předchozím výsledkem, že pravděpodobnost nesouběhu je 52 %.

Pro mnohem vyšší hodnoty (které jsou zajímavé v kryptografických metodách, které se používají v šifrované komunikaci a kryptoměnách) např. $k = 2^{130}$ a $n = 2^{256}$ náš odhad dá

$$\log P = -\frac{1}{2}\frac{k^2}{n} = -\frac{1}{2}\frac{2^{260}}{2^{256}} = -8$$

a pravděpodobnost nesouběhu je

$$P = e^{-8} \doteq 0.000335463$$

a pravděpodobnost souběhu je

$$1 - P = 0.999665.$$

Zdůrazněme, jak by bylo obtížné vyčíslit výraz

$$P = \frac{2^{130}!}{(2^{256} - 2^{130})! (2^{256})^{2^{130}}}.$$

6.1.2019

Pavel.Pokorny@vscht.cz