

**Tvrzení:** Neexistuje algoritmus, který by dokázal bez ztráty informace komprimovat všechny bitové řetězce délky  $n$  alespoň o jeden bit.

**Důkaz:** Předpokládejme, že takový algoritmus existuje. Různých bitových řetězců délky  $n$  je  $2^n$ . Označme si  $x$  počet všech různých řetězců délky nejvýše  $n - 1$ :

$$\begin{aligned}x &= 2^{(n-1)} + 2^{(n-2)} + \dots + 2^{(n-n)} = 2^n 2^{-1} + 2^n 2^{-2} + \dots + 2^n 2^{-n} = \\ &= 2^n (1/2 + 1/4 + \dots + 1/2^n) = 2^n (1 - 2^{-n}) = 2^n - 1\end{aligned}$$

Tedy bitových řetězců maximální délky  $n - 1$  je  $2^n - 1$ . Máme tedy  $2^n$  původních (nekomprimovaných) bitových řetězců a nejvýše  $2^n - 1$  možných komprimovaných řetězců. To ovšem podle Dirichletova principu<sup>1</sup> znamená, že alespoň dva z komprimovaných řetězců jsou stejné, byť vznikly z řetězců různých. To je ve sporu s tím, že nedochází ke ztrátě informace.

□

---

<sup>1</sup>V angličtině poněkud méně rigorózně *Pigeon hole principle*, v jednoduchosti říká, že pokud máte pět holubů a čtyři díry, musíte do jedné díry strčit holuby dva.