Definice 1 *Rozlišující systém je množina M posloupností znaků 0,1 taková, že pro každé dvě různé posloupnosti $a = (a_1, \ldots, a_k)$ a $b = (b_1, \ldots, b_\ell)$ z množiny M existuje i, $0 \leq i \leq \min(k, \ell)$ takové, že $a_i \neq b_i$.*

Je-li M rozlišující systém, pak označíme jako $|M|$ počet prvků množiny M a jako $||M||$ součet délek všech posloupností z M.

Lemma 2 *Je-li M neprázdný rozlišující systém, pak $||M|| \geq |M| \log_2 |M|$.*

Důkaz: Jestliže M obsahuje jednu posloupnost, pak $||M|| \geq 0 = 1 \cdot \log_2 1 = |M| \log |M|$.

Nechť M obsahuje více posloupností. Podle definice pak prázdná posloupnost nemůže být prvkem M, každá posloupnost z M tedy začíná buď 0 nebo 1.

Nechť lemma platí pro všechny rozlišující systémy s menším počtem prvků než M. Jestliže všechny posloupnosti z M začínají stejným symbolem, pak zkrátíme-li je o tento první symbol, dostaneme zase rozlišující systém, který má stejně posloupností, ale menší součet jejich délek. Stačí proto lemma dokázat za předpokladu, že posloupnosti z M nezačínají všechny stejně.

Označme M_0 množinu posloupností z M, které začínají symbolem 0 a jako M_1 množinu posloupností z M, které začínají symbolem 1. Označme jako N_0 (resp. N_1) množinu posloupností, které vzniknou z M_0 (resp. M_1) odtržením počátečního symbolu 0 (resp. 1). Obě množiny N_0 a N_1 jsou neprázdné rozlišující systémy a mají menší počet posloupností než M, lemma pro ně z indukčního předpokladu platí. Označme $|M| = m$, $|M_0| = k$. Pak je $|N_0| = |M_0| = k$, $|N_1| = |M_1| = m - k$ a platí

$$\begin{aligned} ||M|| = ||M_0|| + ||M_1|| = (k + ||N_0||) + (m - k + ||N_1||) \geq \\ \geq m + |N_0| \log_2 |N_0| + |N_1| \log_2 |N_1| \geq \\ \geq m + k \log_2 k + (m - k) \log_2 (m - k). \end{aligned}$$

Snadno se zjistí, že funkce $f(x) = m + x \log_2 x + (m - x) \log_2 (m - x)$ nabývá na $[1, m - 1]$ minima pro $x = m/2$ a proto

$$\begin{aligned} ||M|| \geq m + (n/2) \log_2 (m/2) + (m/2) \log_2 (m/2) = \\ = m + m \log_2 (m/2) = m + m(\log_2 m - 1) = m \log_2 m. \end{aligned}$$

♣

Věta 3 *Je-li $\mathcal{A}$ porovnávací algoritmus, pak průměr přes všechny permutace π množiny $\{1, \ldots, n\}$ z počtu porovnání, které $\mathcal{A}$ potřebuje pro setřídění posloupnosti $\pi(1), \ldots, \pi(n)$ je alespoň $\log_2 (n!)$.*

Důkaz: Pro každou permutaci vypíšeme do posloupnosti výsledky všech porovnání, které algoritmus provedl při třídění posloupnosti $\pi(1), \ldots, \pi(n)$ tak, že zapíšeme 1 za úspěšný test a 0 za neúspěšný test. Je zřejmé, že takto dostaneme rozlišující systém s $n!$ prvky, který tedy má podle předchozího lemmatu průměrnou délku posloupnosti (tedy průměrný počet porovnání) roven $\log_2 (n!)$. ♣

Poznámka. Podle Stirlingova odhadu je

$$n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$$

a tedy

$$\log_2(n!) \approx n \log_2 n - n \log_2 e + 0.5 \cdot \log_2 n + 0.5 \cdot \log_2(2\pi).$$