# 1 Asymptotické odhady

Cílem této kapitoly je vyložit nejpoužívanější asymptotické odhady omezující možné volby parametrů blokových kódů, z nichž některé platí pouze pro kódy lineární. Omezíme se pouze na kódy binární, důvody tohoto omezení budou však čistě technické. Pro $q$-ární kódy, kde $q \geq 3$, lze postupovat obdobně, příslušné vzorce ale bývají komplikovanější.

Prvním krokem je sestavení několika pomocných odhadů, které využívají tzv. entropickou funkci. Logaritmus o základu dvě budeme značit lg. Přirozený logaritmus se značí ln. Začneme tím, že připomeneme následující základní vlastnosti logaritmů.

**Lemma 1.1.** *Ať $x \in \mathbb{R}$, $0 < x < 1$. Pak*

*(i)* $\lg 1 = 0$, $\lg 2 = \ln e = 1$,

*(ii)* $\lg x = \ln x \lg e$ *a* $(\lg x)' = (\lg e)/x$,

*(iii)* $(x \lg x)' = \lg x + \lg e = \lg(ex)$,

*(iv)* $((1-x)\lg(1-x))' = -\lg(1-x) - \lg e = -\lg(e(1-x))$, *a*

*(v)* $\lim_{x\to 0} x \lg x = 0$.

□

*Entropickou funkci* $H$ definujeme pro $\alpha \in (0,1)$ vztahem

$$H(\alpha) = \alpha \lg \tfrac{1}{\alpha} + (1-\alpha) \lg \tfrac{1}{1-\alpha} = -\alpha \lg \alpha - (1-\alpha)\lg(1-\alpha).$$

Z Lemmatu 1.1 plyne, že $\lim_{x\to 0} H(x) = 0 = \lim_{x\to 1} H(x)$. Proto je možné $H$ spojitě dodefinovat v krajních bodech intervalu jako $H(0) = H(1) = 0$. Následující lemma uvádíme bez důkazu, neboť ten plyne z Lemmatu 1.1 přímočarým způsobem.

**Lemma 1.2.** *Entropická funkce $H$ je spojitě definovaná na intervalu $[0,1]$ a má tyto vlastnosti:*

*(i)* $H(\alpha) = H(1-\alpha)$ *pro každé* $\alpha \in [0,1]$, *takže $H$ je symetrická podle osy* $x = 1/2$.

*(ii) Pro každé* $\alpha \in (0,1)$ *platí* $H'(\alpha) = -\lg(\alpha) + \lg(1-\alpha)$, *takže $H$ je rostoucí na intervalu* $[0,1/2]$ *a klesající na intervalu* $[1/2,1]$.

*(iii)* $H'(1/2) = 0$ *a* $H(1/2) = 1$.

□

**Lemma 1.3.** *Ať $n \geq 1$ je celé. Pro každé reálné $r \in (0,n)$ platí*

$$2^{nH(\frac{r}{n})} = \frac{n^n}{r^r (n-r)^{(n-r)}}.$$

*Důkaz.* Z $1 - \frac{r}{n} = \frac{n-r}{n}$ plyne

$$nH(\tfrac{r}{n}) = n\tfrac{r}{n}\lg(\tfrac{n}{r}) + n\tfrac{n-r}{n}\lg(\tfrac{n}{n-r}) = \lg(\tfrac{n}{r})^r + \lg(\tfrac{n}{n-r})^{n-r} = \lg\frac{n^r n^{n-r}}{r^r(n-r)^{n-r}} = \lg\frac{n^n}{r^r(n-r)^{n-r}}.$$

□

Připomeňme, že $V(n,r)$ značí objem (tedy počet prvků) $n$-rozměrné koule s poloměrem $r$ počítané v Hammingově vzdálenosti.

**Lemma 1.4.** *Ať $n$ a $r$ jsou celá čísla, $0 \le r \le n/2$. Pak $V(n,r) = \sum_{i=0}^{r}\binom{n}{i} \le 2^{nH(r/n)}$. Je-li $r > 0$, platí tato nerovnost jako ostrá.*

*Důkaz.* Z $r \le n/2$ plyne $r/(n-r) \le 1$. Tudíž $1 \ge (\frac{r}{n-r})^{r-i}$, a tedy $r^i(n-r)^{n-i} \ge r^r(n-r)^{n-r}$ pro každé $i \ge 0$. Proto

$$n^n = (r + (n-r))^n = \sum_{i=0}^{n}\binom{n}{i}r^i(n-r)^{n-i} \ge \sum_{i=0}^{r}\binom{n}{i}r^n(n-r)^{n-r}.$$

Poslední nerovnost platí jako ostrá, pokud $r > 0$, neboť pak jsou vypouštěné členy nenulové. Zbytek plyne z Lemmatu 1.3. □

Uvedené důkazy pracují s poměrně velkoryse koncipovanými odhady. Pro důkazy asymptotických vztahů se takové odhady však ukazují jako dostačující. Pro práci s faktoriály proto také nebudeme využívat Stirlingovy formule

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

ale spokojíme se s odhadem

$$\left(\frac{n}{e}\right)^n < n! \text{ pro } n \ge 0 \text{ a } n! < \left(\frac{n}{e}\right)^{n+1} \text{ pro } n \ge 50,$$

který je možné dokázat elementárně (což zde činit ovšem nebudeme).

**Lemma 1.5.** *Jsou-li $n$ a $k$ celá čísla, přičemž $k \ge 50$ a $n - k \ge 50$, tak platí*

$$\binom{n}{k} > 2^{nH(\frac{k}{n})}\frac{e^2}{k(n-k)}.$$

*Důkaz.* Z uvedeného odhadu výpočtu faktoriálu máme

$$\frac{n!}{k!(n-k)!} > \frac{n^n}{k^{k+1}(n-k)^{n-k+1}}\cdot\frac{e^{k+1}e^{n-k+1}}{e^n} = \frac{n^n}{k^k(n-k)^{n-k}}\cdot\frac{e^2}{k(n-k)}.$$

Zbytek plyne z Lemmatu 1.3. □

*Informační poměr* neboli *nosnost* $\alpha(C)$ binárního $(n, k, d)$ kódu $C$ se definuje jako $(\lg k)/n$. Pro $[n, k, d]$ kód $C$ je tedy $\alpha(C) = k/n$.

*Relativní vzdáleností* se rozumí poměr $d/n$.

Ať $\mathcal{C}$ je nějaká třída sestávající se z nekonečně mnoha různých binárních kódů. Řekneme o ní, že je *asymptoticky dobrá,* jestliže existují konstanty $\alpha_0$ a $\delta_0$ takové, že

$$\alpha(C) > \alpha_0 > 0 \text{ a } \delta(C) > \delta_0 > 0 \text{ pro všechna } C \in \mathcal{C}.$$

Mnohé standardně studované třídy binárních kódů asymptoticky dobré nesou. U jiných odpověď není známa. Asymptoticky dobré třídy binárních kódů však existují a jsou známy. Jejich konstrukce bývá založena na iterativních postupech, kterým jsme se zde nevěnovali.

Pro $n \geq d \geq 1$ definujme $A(n, d)$ jako maximum ze všech hodnot $\lg k$ takových, že existuje $(n, k, d)$ kód.

Poměr $A(n, d)/n$ tedy udává nejvyšší možnou nosnost při zadané délce a minimální vzdálenosti. Limitním přechodem pak dostáváme asymptotickou nosnost při zadané relativní vzdálenosti, a to vztahem

$$\alpha(\delta) = \limsup_{n\to\infty} \frac{A(n, \lceil \delta n \rceil)}{n}.$$

**Lemma 1.6.** *Ať $1 \leq d \leq n/2$. Potom $A(n, d) \geq n(1 - H(\frac{d-1}{n}))$, přičemž pro $d > 1$ platí ostrá nerovnost.*

*Důkaz.* Případ $d = 1$ vede na totální kód a je zřejmý. Proto lze předpokládat $d > 1$. Podle Lemmatu 1.4 je $\lg V(n, d-1) < nH(\delta)$, kde $\delta = (d-1)/n$. Z Tvrzení **??** tedy víme, že $[n, k, d]$ kód existuje, jestliže $nH(\delta) \leq n - k + 1$. Podmínku $k \leq n(1 - H(\delta)) + 1$ splňuje alespoň jedno celé $k \geq n(1 - H(\delta))$, a proto $A(n, d) \geq k \geq n(1 - H(\delta))$. □

Můžeme tudíž vyslovit tzv. *asymptotický Gilbert-Varšamovův odhad:*

**Tvrzení 1.7.** *Ať $0 < \delta \leq 1/2$. Pak $\alpha(\delta) \geq 1 - H(\delta)$.*

*Důkaz.* Podle Lemmatu 1.6 pro dostatečně velké $n$

$$\frac{A(n, \lceil \delta n \rceil)}{n} > 1 - H\left(\frac{\lceil \delta n \rceil - 1}{n}\right),$$

takže pro dokončení důkazu stačí ověřit nerovnost $\frac{\lceil \delta n \rceil - 1}{n} \leq \delta$, neboť funkce $H$ je na intervalu $[0, 1/2]$ podle Lemmatu 1.2 rostoucí. Platnost nerovnosti vyplývá z toho, že ji lze vyjádřit jako $\lceil \delta n \rceil \leq \delta n + 1$. □

Protipólem k předchozímu odhadu je tzv. *asymptotický Hammingův odhad:*

**Tvrzení 1.8.** *Pro každé $\delta$, $0 < \delta < 1$, platí $\alpha(\delta) \leq 1 - H(\delta/2)$.*

*Důkaz.* Pro každé $n \geq 8$ položme $\mu(n) = \max\{|\lg e^2 - \lg r - \lg(n-r)|;\ 0 < r < n\}$. Zjevně $\mu(n) \leq 2\lg n$, takže $\lim_{n\to\infty} \mu(n)/n = 0$. Členy asymptotických odhadů, které limitně míří k nule, je zvykem označovat $o(1)$. Podle lemmat 1.4 a 1.5 máme $V(n,r) > \binom{n}{r} > 2^{nH(r/n)} e^2 r^{-1}(n-r)^{-1}$ pro všechna celá $r$ a $n$, která splňují $r \geq 50$ a $n \geq r + 50$. Proto v takovém případě $\lg V(n,r) > \lg \binom{n}{r} > nH(\frac{r}{n}) + \lg e^2 - \lg r - \lg(n-r)$, takže $\frac{\lg V(n,r)}{n} > H(\frac{r}{n}) + o(1)$.

Z Hammingova odhadu víme, že kódy s minimální vzdáleností $d \geq 2r+1$ mají méně než $2^n/V(n,r)$ prvků. Z $[\frac{\delta n-1}{2}] \leq \frac{\delta n-1}{2}$ plyne $2[\frac{\delta n-1}{2}] + 1 \leq \lceil \delta n \rceil$, takže

$$\frac{A(n, \lceil \delta n \rceil)}{n} \leq \frac{1}{n} \lg \left( \frac{2^n}{V(n, [\frac{\delta n-1}{2}])} \right) = 1 - \frac{\lg V(n, [\frac{\delta n-1}{2}])}{n}$$
$$< 1 - H\left( \frac{[\frac{\delta n-1}{2}]}{n} \right) - o(1).$$

Zbytek plyne z limitního přechodu, Lemmatu 1.2 a nerovností

$$\frac{1}{2} > \frac{1}{n}\left[\frac{\delta n - 1}{2}\right] > \frac{\delta n - 1}{2n} = \frac{\delta}{2} - \frac{3}{2n}.$$

□