Eliasův-Bassalygův odhad v teorii samoopravných kódů

Jiří Matoušek (KAM MFF UK)

Verze: 14/XII/2008

Tento text víceméně navazuje na text Tomáše Kaisera o samoopravných kódech, viz `http://home.zcu.cz/~kaisert/kody/kody.pdf`, speciálně na kapitolu 10, v níž je vyložen asymptotický Gilbertův-Varshamovův dolní odhad a Hammingův horní odhad.

Zde uvažujeme binární kódy C délky n nad abecedou $S = \{0, 1\}$ s minimální vzdáleností $d = d(C)$. Definujeme *relativní vzdálenost* kódu C jako $\delta(C) := d/n$ a *hustotu* C jako

$$\rho(C) := \frac{\log_2 |C|}{n}$$

(zde se naše značení liší od Kaiserova). Dále pro stručnost vyjadřování zavedeme funkci $\rho_{\max}\colon [0, 1] \to [0, 1]$:

$$\begin{aligned}\rho_{\max}(\delta) \quad := \quad \sup \Big\{ \rho : & \text{ pro nekonečně mnoho } n \text{ existuje kód } C \text{ délky } n \\ & \text{splňující } \delta(C) \geq \delta \text{ a } \rho(C) \geq \rho \Big\}.\end{aligned}$$

V textu Tomáše Kaisera jsou dokázány následující asymptotické odhady:

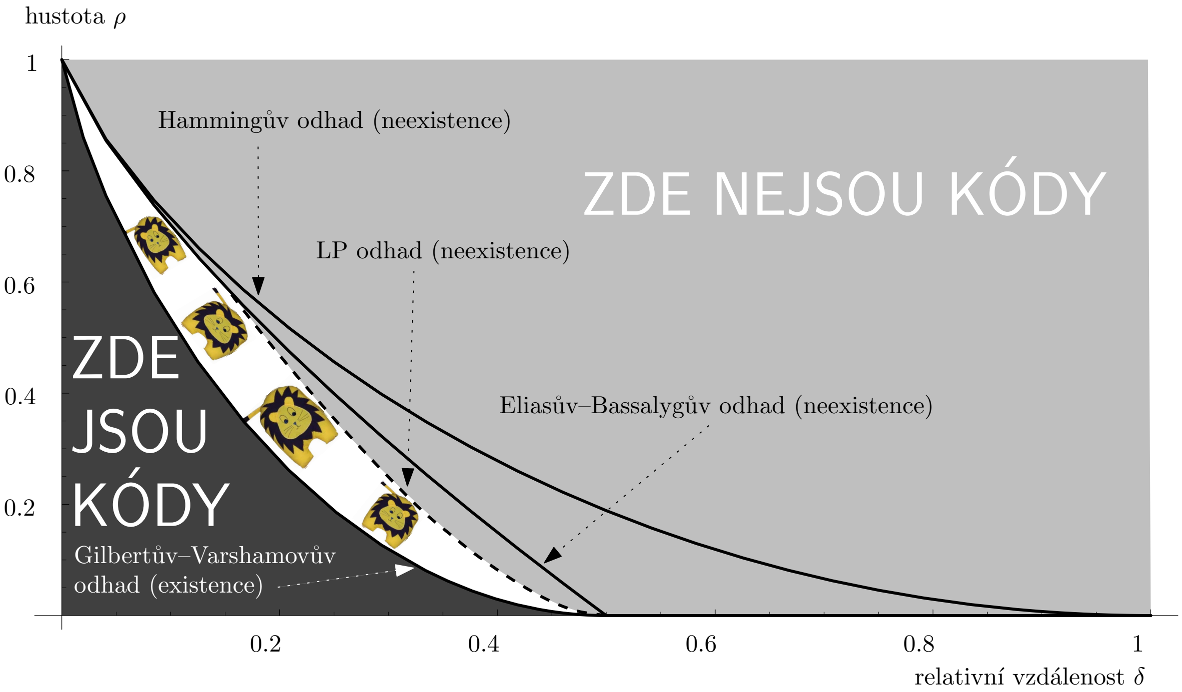
- (Gilbert-Varshamov)
$$\rho_{\max}(\delta) \geq 1 - H(\delta), \quad 0 \leq \delta \leq \frac{1}{2},$$

- (Hamming)
$$\rho_{\max}(\delta) \leq 1 - H(\delta/2), \quad 0 \leq \delta \leq 1,$$

kde $H(x) := -x \log_2 x - (1-x) \log_2(1-x)$. Zde ukážeme hlavní kroky důkazu lepšího horního odhadu:

- (Elias-Bassalygo)
$$\rho_{\max}(\delta) \leq 1 - H\left(\frac{1 - \sqrt{1 - 2\delta}}{2}\right), \quad 0 \leq \delta \leq \frac{1}{2}.$$

Příslušné funkce jsou znázorněny na následujícím obrázku, spolu s dalším dolním odhadem (LP-odhad neboli odhad Delsarteovou metodou pomocí lineárního programování), o němž zde nic dalšího neřekneme.



Z důkazu Eliasova-Bassalygova odhadu uvedeme jenom hlavní část – vynecháme asymptotické počítání, z něhož by se dostal uvedený vzorec.

Na Eliasův-Bassalygův odhad se dá pohlížet jako na vylepšení Hammingova odhadu. V Hammingově odhadu jsme do „prostoru" S^n všech možných slov délky n umisťovali disjunktní koule kolem kódových slov a v takovém případě jsme si mohli dovolit poloměr $r := \lfloor (d-1)/2 \rfloor$, zhruba polovinu minimální vzdálenosti. Celkový objem všech koulí nemohl být větší než 2^n, a odtud jsme dostali Hammingův odhad $|C| \leq 2^n / V(n,r)$, kde $V(n,r) = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{r}$ je počet slov v Hammingově kouli o poloměru r v S^n.

Zde uděláme koule větší, takže se budou moct překrývat, ale dáme pozor, aby se nepřekrývaly příliš mnoho. Když se podaří zajistit, aby žádné slovo z S^n nebylo obsaženo ve více než K z těchto koulí, potom součet jejich objemů nemůže být větší než $2^n K$. To formálně vyjádříme v následujícím lemmatu.

Lemma 1 (Pakování koulí s omezeným překryvem) *Nechť C je binární kód délky n a předpokládejme, že pro každé slovo $x \in S^n$ platí $|B(x,t) \cap C| \leq K$ (tj. libovolná koule o poloměru t obsahuje nejvýš K kódových slov), kde K a t jsou nějaká přirozená čísla. Potom*

$$|C| \leq \frac{2^n K}{V(n,t)}.$$

Důkaz. Uvažme systém koulí $\{B(w,t) : w \in C\}$. Podle předpokladu je každé slovo $x \in S^n$ obsaženo v nejvýš K koulích z tohoto systému. Proto $\sum_{w \in C} |B(w,t)| = |C| \cdot V(n,t) \leq 2^n K$. □

Čím větší uděláme poloměr t v tomto lemmatu, tím více se budou koule překrývat. Jak roste t, roste $V(n,t)$, ale roste také K, a tyto dvě tendence působí v odhadu proti sobě, takže musíme najít vhodný kompromis. Jádrem Eliasova-Bassalygova odhadu je poznatek, že až do určité vhodné hodnoty t roste K jen pomalu, polynomiálně, kdežto $V(n,t)$ roste mnohem rychleji, zhruba exponenciálně.

Lemma 2 *Nechť C je binární kód délky n a minimální vzdálenosti d, a nechť $t \le \frac{n}{2}$ a K jsou přirozená čísla, splňující*

$$2t\left(1 - \frac{t}{n}\right) < d\left(1 - \frac{1}{K}\right).$$

Potom $|B(x,t) \cap C| < K$ pro libovolnou kouli $B(x,t)$ o poloměru t.

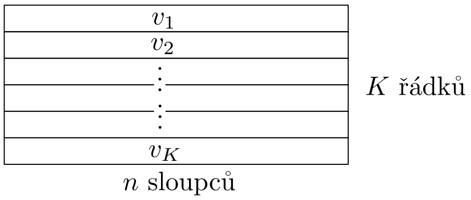
Numerický příklad. Z kombinace Lemmatu 1 a 2 se dá spočítat Eliasův-Bassalygův odhad pro $\rho_{\max}(\delta)$, uvedený na začátku. Zde to dělat nebudeme a místo toho ukážeme použití lemmat aspoň pro konkrétní číselné hodnoty parametrů.

Vezměme třeba $\delta = 0{,}4$ a $n = 1000$. Kód délky 1000 s relativní vzdáleností 0,4 má $d = 400$, a poloměr koulí v Hammingově odhadu je tedy $r = 199$. Zvolme v Lemmatu 2 číslo t tak velké, aby $2t(1 - \frac{t}{n})$ bylo jen o málo menší než d – největší použitelné t je 276 (což je zhruba 1,4-krát větší než r), pro nějž $2t(1 - \frac{t}{n}) = 399{,}648$. Pak stačí zvolit $K = 1137$ a nerovnost v Lemmatu 2 je splněna, takže žádná koule o poloměru 276 neobsahuje víc než 1136 kódových slov. Tudíž nám Lemma 1 dá nerovnost $|C| \le 2^{1000} 1036/V(1000, 276)$, z níž můžeme numericky vypočítat, že $\rho(C) \le 0{,}164533$ (z Hammingova odhadu vyjde pouze $\rho(C) \le 0{,}284651$). (Pro zvídavější čtenáře: Zkuste numericky zjistit, jestli tato volba t je optimální, nebo jestli pro některé menší t bychom dostali ještě lepší odhad na $|C|$.)

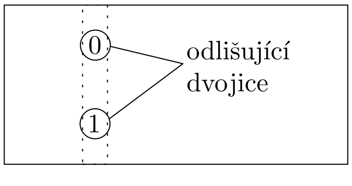
Důkaz Lemmatu 2. Pro spor předpokládejme, že existuje koule $B(x,t)$ obsahující K kódových slov $w_1, w_2, \ldots, w_K$. Podle předpokladů máme $d(w_i, w_j) \ge d$ pro každé $i \ne j$ a také $d(x, w_i) \le t$ pro každé i, kde $d(u,v)$ značí Hammingovu vzdálenost slov u a v, tj. v kolika pozicích se liší.

Pro zjednodušení definujme nová slova $v_i := w_i - x$, kde slova odečítáme jako vektory nad dvouprvkovým tělesem, tj. modulo 2 (připomeňme, že abeceda je $S = \{0, 1\}$). Je snadno vidět, že z $d(w_i, w_j) \ge d$ plyne $d(v_i, v_j) \ge d$ a že z $d(x, w_i) \le t$ plyne $d(0, v_i) \le t$ – čili že žádné v_i nemá víc než t jedniček.

Napišme teď slova $v_1, v_2, \ldots, v_K$ do tabulky s n sloupci a K řádky, kde v i-tém řádku je slovo v_i:



Definujme *odlišující dvojici* jako (neuspořádanou) dvojici políček v tabulce, z nichž jedno obsahuje 1 a druhé 0 a která leží ve stejném sloupci:



Jádrem důkazu je počítání odlišujících dvojic dvěma způsoby. Poněvadž se každé dva řádky tabulky liší aspoň v d sloupcích, musí v tabulce být přinejmenším $\binom{K}{2}d$ odlišujících dvojic. Na druhé straně označíme-li počet jedniček v i-tém sloupci písmenem j_i, potom tento sloupec obsahuje $K - j_i$ nul a přispívá tedy $j_i(K - j_i)$ odlišujícími dvojicemi. Proto

$$\binom{K}{2} d \leq \sum_{i=1}^{n} j_i(K - j_i). \tag{1}$$

Čísla j_i neznáme, ale protože každý řádek má nejvýš t jedniček, víme, že celkový počet jedniček v tabulce splňuje

$$\sum_{i=1}^{n} j_i \leq Kt.$$

Označíme ještě $\sum_{i=1}^{n} j_i$ písmenem J. Odhadneme teď pravou stranu klíčové nerovnosti (1) výrazem, který už na číslech j_i záviset nebude. Použijeme Cauchyho-Schwarzovu nerovnost, která pro reálná čísla $x_1, x_2, \ldots, x_n$ a $y_1, y_2, \ldots, y_n$ říká $(\sum_{i=1}^{n} x_i y_i)^2 \leq (\sum_{i=1}^{n} x_i^2)(\sum_{i=1}^{n} y_i^2)$. My do ní dosadíme $x_i = j_i$ a $y_i = 1$ a dostaneme

$$\sum_{i=1}^{n} j_i^2 \geq \left(\sum_{i=1}^{n} j_i\right)^2 / n = \frac{J^2}{n}.$$

Pak spočítáme

$$\sum_{i=1}^{n} j_i(K - j_i) = K\left(\sum_{i=1}^{n} j_i\right) - \sum_{i=1}^{n} j_i^2 \leq KJ - \frac{J^2}{n} = J\left(K - \frac{J}{n}\right).$$

Nyní je potřeba si všimnout, že funkce $x \mapsto x(K - x/n)$ je rostoucí pro $x \leq Kn/2$ (kdo nevěří, ať derivuje). Z předpokladu $t \leq \frac{n}{2}$ v lemmatu a z nerovnosti $J \leq Kt$ máme $J \leq Kt \leq Kn/2$, a tedy $J(K - J/n) \leq Kt(K - Kt/n) = K^2 t(1 - \frac{t}{n})$.

Připomeňme, že toto je horní odhad pro pravou stranu nerovnosti (1), takže celkem jsme dospěli k nerovnosti

$$\binom{K}{2} d = \frac{K(K-1)}{2} d \leq K^2 t \left(1 - \frac{t}{n}\right),$$

čili po vynásobení $2/K^2$

$$d\left(1 - \frac{1}{K}\right) \leq 2t\left(1 - \frac{t}{n}\right).$$

To je přesně opačná nerovnost, než předpokládáme v lemmatu. Dostáváme tak spor s předpokladem, že nějaká koule o poloměru t obsahovala K (nebo víc) kódových slov, a tím je lemma dokázáno. $\square$

Poděkování. Za pročtení předběžné verze a drobné opravy děkuji Zuzaně Safernové a Bernardu Lidickému.