$V(n,r)$ je objem Hammingovy koule poloměru r v dim. n. $V(n,r) = \sum_{i=0}^{r} \binom{n}{i}$. Pokud $0 < r \leq \frac{n}{2}$,

pak $V(n,r) \leq 2^{n H(\frac{r}{n})}$

Dk: ozn $p := \frac{r}{n}$

$$\cdot \left(\frac{1}{2}\right)^{H(p)n} = \left(\frac{1}{2}\right)^{n\left(p \lg \frac{1}{p} + (1-p)\lg(1-p)\right)} = \left(\frac{1}{2}\right)^{-\left(\lg\left(p^{pn}\right) + \lg\left((1-p)^{(1-p)n}\right)\right)} =$$

$$p^{pn} \cdot (1-p)^{n(1-p)}$$

$$\cdot \mathrm{Vol}(n, p^n) = \sum_{i=0}^{pn} \binom{n}{i}$$

$$1 = (p + (1-p))^n$$

$$= \sum_{i=0}^{n} \binom{n}{i} p^i (1-p)^{n-i} \qquad \text{binom. věta}$$

$$= \sum_{i=0}^{pn} \binom{n}{i} p^i (1-p)^{n-i} + \sum_{i=pn+1}^{n} \binom{n}{i} p^i (1-p)^{n-i}$$

$$\geq \sum_{i=0}^{pn} \binom{n}{i} p^i (1-p)^{n-i} \qquad \text{zahodíme} \nearrow$$

$$= \sum_{i=0}^{pn} \binom{n}{i} p^i (1-p)^{n-i} \frac{(1-p)^i}{(1-p)^i} \qquad \text{rozšíříme jedničkou} = \left(\frac{1-p}{1-p}\right)^i$$

$$= \sum_{i=0}^{pn} \binom{n}{i} \left(\frac{p}{1-p}\right)^i (1-p)^n$$

$$\geq \sum_{i=0}^{pn} \binom{n}{i} \left(\frac{p}{1-p}\right)^{pn} (1-p)^n \qquad p \leq \frac{1}{2} \to \frac{p}{1-p} \leq 1 \to \left(\frac{p}{1-p}\right)^i \geq \left(\frac{p}{1-p}\right)^{i+1} \quad \forall i \in \mathbb{N}_0$$

$$= \sum_{i=0}^{pn} \binom{n}{i} p^{pn} (1-p)^{n(1-p)} = \mathrm{Vol}(n, p^n) \cdot 2^{-H(p)n}$$

Gilbert - Varshamov bound

Věta: Pro každé $\delta \in [0, \frac{1}{2})$ existuje rodina bin. kódů $\mathcal{C}$ s $R(\mathcal{C}) \geq 1 - H(\delta)$ a rel. vzdáleností $\delta(\mathcal{C}) \geq \delta$. $\left(\delta = \frac{d}{n}\right)$

Dk algoritmem

1. $\mathcal{C} \leftarrow \emptyset$
2. dokud existuje slovo $u \in \mathbb{Z}_2^n$ t.ž. $\Delta(u, \mathcal{C}) \geq d$:
   3. $\mathcal{C} \leftarrow \mathcal{C} \cup \{u\}$
4. return $\mathcal{C}$

vlastnosti:

- $\bigcup_{u \in \mathcal{C}} B(u, d-1) \supseteq \mathbb{Z}_2^n$ protože jestli u, tak existuje slovo, které je dalek. od $\mathcal{C}$ v $\mathcal{C}$.
- $\sum_{u \in \mathcal{C}} B(u, d-1) \geq \left| \bigcup_{u \in \mathcal{C}} B(u, d-1) \right| \Rightarrow \sum_{u \in \mathcal{C}} B(u, d-1) \geq 2^n$
- explicitně $\rightarrow 2^{O(n)}$ reprezentace
  - jde lépe?

$$\sum_{u \in \mathcal{C}} Vol(u, d-1) \geq 2^n \qquad Vol(u, d-1) \leq Vol(u, \delta)$$

$$|\mathcal{C}| \geq \frac{2^n}{Vol(u, d-1)} \geq \frac{2^n}{2^{-H(\delta)n}} = 2^{n(1-H(\delta))}$$

- ukážeme, že patřičný kód jde vyrobit náhodně.

Formálně: Pro každé $\varepsilon \in [0, 1 - H(\delta)]$, kde $\delta \in [0, \frac{1}{2}]$ a $n \in \mathbb{N}$, náhodně vybraná matice G z $\mathbb{Z}_2^{k \times n}$, kde $k = n(1 - H(\delta) - \varepsilon)$, je generující matice s $R = 1 - H(\delta) - \varepsilon$ a relativní vzdáleností alespoň δ s pravd. alespoň $1 - 2^{-\varepsilon n}$.

- co vlastně hledáme je matice G t.ž. $w(m \cdot G) \geq d$ pro $\forall m \in \{0,1\}^k \setminus \vec{0}$
- G zvolíme tak, že na každé místě dáme uniformně nezávisle náhodně 0 nebo 1

Tvrzení: $m \cdot G$ je uniformně nezávisle náhodný vektor z $\mathbb{Z}_2^n$

- nezávislost: každý prvek $b = m \cdot G$ je vyjádřen $b_i = \sum_{j=1}^{k} m_j G_{ji}$ jiného sloupce

· rovnomocnost: bíno $m_1 \neq 0$. Zafixujeme-li výsledek $\sum_{j=2}^{l} m_j G_j$, tak právě jedna volba $m_1 G_1$ zajistí, že b_i je právě nějaké číslo.

$$\rightarrow Pr[w(m \cdot G) < d] = \frac{Vol(n, d-1)}{2^n} \leq \frac{2^{H(\delta) n}}{2^n} = 2^{-n(1-H(\delta))} \leq 2^{-k} \cdot 2^{-\varepsilon n}$$

$k \leq 1 - H(\delta) - \varepsilon$

· union bound přes nenulová zprávy

$$Pr[\exists m: w(mG) < d] \leq (2^k - 1)(2^{-k} \cdot 2^{-\varepsilon n}) < 2^{-\varepsilon n}$$

· jistě potřebujeme ukázat, že $rank(G) = k$

· $rank(G) < k \Rightarrow$ existuje nenulová LK řádků, které se sečtou na 0

· tyto koeficienty dojde do nenulového vektoru z

· $zG = \vec{0}$ a $z \neq \vec{0} \Rightarrow w(zG) = 0 < d$ ↯

· $\varepsilon = 0 \Rightarrow$ pst úspěchu je $\geq \frac{1}{2}$

· $\varepsilon > 0 \Rightarrow$ — " — $1 - \left(\frac{1}{2}\right)^{\varepsilon \cdot n}$

Singleton bound

Věta: Pro l.k. (n, k, d) - kód platí $k + d \leq n + 1$.

Dk:

- nechť $u_1, \dots, u_M$ jsou kódová slova
- chceme ukázat $M \leq 2^{n-d+1}$
- nechť u_i' je prefix slova u_i délky $n-d+1$
- tvrdíme, že $u_i' \neq u_j'$ pro všechna $i \neq j$
- pro spor nechť to neplatí, tj. existují i, j t.ž. $u_i' = u_j'$
- pak ale $\Delta(u_i, u_j) \leq n - n + d - 1 = d - 1$
- spor s předpokladem, že Δ_{min} je d

$\rightsquigarrow$ M je # různých prefixů $\rightarrow$ $M \leq 2^{n-d+1}$

Nechť $x, y \in \{0,1\}^*$. Ukažte, že $K(x,y) \leq K(x) + K(y) + c$ pro nějakou konst. c.

- uděláme univ. program
  1. zavolej program pro x, ten musí existovat
  2. — " — y

Chceme konstr. černobílé obrázky velikosti $n \times n$. Máme tedy n^2 pixelů, barvy je černý či bílý. n je konst, pro naše programy můžeme předpokládat, že n je nějaká zakódováno.

a) K(vodorovná čára v i-tém řádku?)

b) K(čtverec)?

c) K()?

a)
- pgm dostane na vstupu i:

```
for j in [n]:
    M[i][j] ← 1
```

$K(\square) \leq \lg n + c$

b)
- pgm dostane na vstupu horní levý roh a délku strany čtverce

$K(\square) \leq \lg n + \lg n + c$
(x souřadnice, y souřadnice, délka strany)

c)
- pgm dostane na vstupu řádek a sloupec

$K(\square) \leq 2 \lg n + c$