応用数学５ 2010 年 6 月 22 日

符号の限界式

講師: 安永憲司

符号の限界式の議論に戻る．ここでは，符号のレートの上界を，相対最小距離の関数として与えることを考える．まず，具体的な限界式を与え，それをもとに漸近的な限界式を与えるということを行う．

これまで見てきた限界式として，Gilbert-Varshamov 限界と Hamming 限界がある．Gilbert-Varshamov 限界は，符号長 n，最小距離 d の二元符号として，符号語数が $\frac{2^n}{\mathrm{Vol}(n,d-1)}$ 以上のものが存在することを保証している．漸近的な表現にすると，相対最小距離が δ のとき，レートが $1-H(\delta)$ に近づくような符号が存在することを示している．一方，Hamming 限界は，符号語数の上界を与えている．符号長 n，最小距離 d の二元符号は，符号語数が必ず $\frac{2^n}{\mathrm{Vol}(n,\lfloor (d-1)/2 \rfloor)}$ 以下になることを示している．漸近的な表現にすると，相対最小距離が δ のとき，レートは $1-H(\delta/2)+\mathrm{o}(1)$ 以下でなければならないことを示している．

1 Singleton 限界

定理 1 (Singleton 限界) 符号長 n, 最小距離 d，アルファベットサイズ q の符号 C に対して，$|C| \leq q^{n-d+1}$.

証明: 矛盾を導くため, $|C| > q^{n-d+1}$ であると仮定する．鳩の巣原理より，ある二つの符号語 $c_1, c_2 \in C, c_1 \neq c_2$ が存在し，これらの符号語は最初の $n-d+1$ シンボルが一致している．すると，$d(c_1,c_2) \leq d-1 < d$ であり，C の最小距離が d であることに矛盾する．■

系 2 (漸近的 Singleton 限界) レート R，相対最小距離 δ の符号に対して，$R \leq 1-\delta+\mathrm{o}(1)$.

Singleton 限界を達成する符号は存在する．Reed-Solomon 符号がその一つであり，最小距離 d のとき，次元が $n-d+1$ である．一般に，Singleton 限界を達成する符号を最大距離分離 (maximum distance separable, MDS) 符号と呼ぶ．

しかしながら，Reed-Solomon 符号などの最大距離分離符号は，アルファベットサイズが符号長にしたがって大きくなる必要がある．アルファベットサイズが固定された符号，例えば二元符号、に対しては，Singleton 限界を改良することができる．

2 Plotkin 限界

定義 3 ベクトル $x, y \in \mathbb{R}^n$ に対し，x と y の内積は $\langle x,y \rangle = \sum_{i=1}^n x_i y_i$ である．ベクトル x のノルムは $\|x\| = \sqrt{\langle x,x \rangle}$ である．

補題 4 ベクトル $v_1, \ldots, v_m \in \mathbb{R}^n$ を考える．

1. $v_1, \ldots, v_m$ が単位ベクトル (つまり，$\|v_i\| = 1$) であり，$\epsilon > 0$ に対して，すべての $1 \leq i < j \leq m$ が $\langle v_i, v_j \rangle \leq -\epsilon$ を満たすとき，$m \leq 1 + \frac{1}{\epsilon}$.
2. $v_1, \ldots, v_m$ が非零ベクトルであり，すべての $1 \leq i < j \leq m$ が $\langle v_i, v_j \rangle \leq 0$ を満たすとき，$m \leq 2n$.

証明: 一つ目について,

$$0 \leq \left\langle \sum_{i=1}^{m} v_i, \sum_{i=1}^{m} v_i \right\rangle = \sum_{i=1}^{m} \|v_i\|^2 + 2 \sum_{1 \leq i < j \leq m} \langle v_i, v_j \rangle \leq m - m(m-1)\epsilon.$$

したがって，$m \leq 1 + 1/\epsilon$.

二つ目は，n についての帰納法によって証明する．基底段階は $n = 0$ のときであり，このとき $m = 0$ なので $m \leq 2n$ は成り立つ．

帰納段階として，$n-1$ 以下ではすべて成り立つと仮定して，n のときに成り立つことを示す．非零ベクトル $v_1, \ldots, v_m \in \mathbb{R}^n$ が，すべての $i \neq j$ に対し，$\langle v_i, v_j \rangle \leq 0$ であるとする．基底の変換を行うことで，$v_m = (1, 0, \ldots, 0)$ であると仮定してもよい．このとき，$1 \leq i \leq m-1$ に対して，v_i を $\alpha_i \in \mathbb{R}, y_i \in \mathbb{R}^{n-1}$ を用いて，$v_i = (\alpha_i, y_i)$ と表すことにする．ただし，$\langle v_i, v_m \rangle \leq 0$ であるので，$\alpha_i \leq 0$ でなければならない．このとき，$y_1, \ldots, y_{m-1}$ の中で，全零ベクトルであるのは一つ以下であることがわかる．なぜならば，もし $y_1 = y_2 = 0$ であったとき，v_1, v_2 は非零ベクトルなので $\alpha_1, \alpha_2 < 0$ である．しかし，$\langle v_1, v_2 \rangle = \alpha_1 \alpha_2 > 0$ であり，矛盾が生じる．次に，一般性を失うことなく，$v_1, \ldots, v_{m-2}$ が非零ベクトルだと仮定する．このとき，すべての $i \neq j \in \{1, \ldots, m-2\}$ に対して，$\langle y_i, y_j \rangle = \langle v_i, v_j \rangle - \alpha_i \alpha_j \leq \langle v_i, v_j \rangle \leq 0$ である．このとき，$n-1$ 次元の非零ベクトル $m-2$ 個に対して，帰納法の仮定を適用すると，$m - 2 \leq 2(n-1)$ でなければならない．したがって，$m \leq 2n$ が導かれる．■

定理 5 (Plotkin 限界) 符号長 n，最小距離 d の二元符号 C に対して以下が成り立つ．

1. $d = n/2$ ならば，$|C| \leq 2n$.
2. $d > n/2$ ならば，$|C| \leq \frac{2d}{2d-n}$

証明: $|C| = m$ とし，$c_1, \ldots, c_m \in \{0,1\}^n$ を C の符号語だとする．仮定より，$1 \leq i < j \leq m$ に対して，$d(c_i, c_j) \geq d$ である．各符号語 c_i を，それぞれが 90 度以上の角度をもつ (つまり，$\langle v_i, v_j \rangle \leq 0$ となる) ように，単位ベクトル $v_i \in \mathbb{R}^n$ へ対応させる．ベクトル v_i は次のように定義される．

$$v_i = \frac{1}{\sqrt{n}}((-1)^{c_{i1}}, (-1)^{c_{i2}}, \ldots, (-1)^{c_{in}})$$

ただし，c_{ij} は c_i の j ビット目を表している．このとき，

$$\langle v_i, v_j \rangle = \frac{1}{n}\left(n - 2d(c_i, c_j)\right) \leq \frac{n-2d}{n}$$

であることがわかる．

もし，$d \geq n/2$ ならば，この内積は 0 以下となり，補題 4 より，$m \leq 2n$ が導かれる．

もし，$d > n/2$ ならば，内積の値は負になり，同じ補題により，

$$m \leq 1 + \frac{n}{2d-n} = \frac{2d}{2d-n}$$

が導かれる．■

上の定理より，相対最小距離が 1/2 以上の二元符号族は，符号語数が $\mathrm{O}(n)$ 以下であることがわかる．これは，相対最小距離が 1/2 以上符号族は，レートが 0 になることを意味している．

次に，相対最小距離が 1/2 未満の場合のレートの上界を示す．

定理 6 (Plotkin 限界) 符号長 n，最小距離 $d < n/2$ の二元符号 C に対して，$|C| \leq d \cdot 2^{n-2d+2}$.

証明: $\ell = n-2d+1, S = \{1, 2, \ldots, \ell\}$ とする．各 $a \in \{0,1\}^\ell$ に対して, C_a を, 最初 ℓ ビットが a に一致するような C の部分集合を $S^c = \{1, 2, \ldots, n\} \backslash S$ へ射影したものとする．つまり, $C_a = \{c_{|S^c} : 1 \leq i \leq \ell \text{に対して } c_i = a_i\}$ と定義する．各 C_a は，符号長 $n-\ell = 2d-1$ の二元符号である．また，C の最小距離が d 以上なので，C_a の最小距離も d 以上である．したがって, 定理 5 より, $|C_a| \leq 2d$. すると, $|C| = \sum_{a \in \{0,1\}^\ell} |C_a| \leq 2d \cdot 2^\ell = d \cdot 2^{n-2d+2}$.
■

系 7 (漸近的 Plotkin 限界) レート R，相対最小距離 δ の二元符号に対して，$R \leq 1 - 2\delta + \mathrm{o}(1)$.

3 まとめ

レート R, 相対最小距離 δ の二元符号は以下を満たす.

$$\text{Hamming :} \quad R \leq 1 - H(\delta/2) + \mathrm{o}(1) \tag{1}$$
$$\text{Singleton :} \quad R \leq 1 - \delta + \mathrm{o}(1) \tag{2}$$
$$\text{Plotkin :} \quad R \leq 1 - 2\delta + \mathrm{o}(1) \tag{3}$$
$$\tag{4}$$

また，以下を満たす符号が存在する.

$$\text{Gilbert-Varshamov :} \quad R \geq 1 - H(\delta) \tag{5}$$

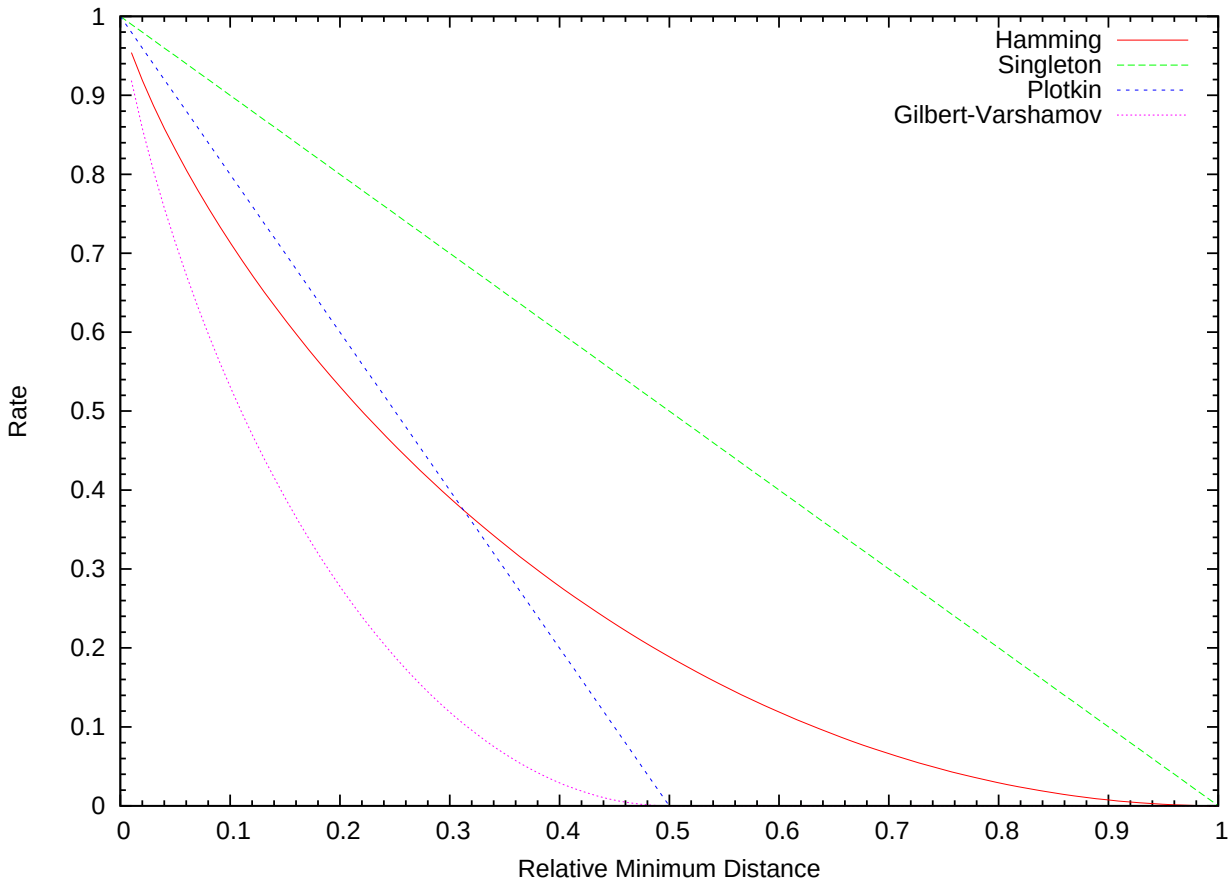

図 1　二元符号に対する限界式