応用数学５ 2010 年 5 月 25 日

Gilbert-Varshamov 限界

講師: 安永憲司

1 漸近記法

あるパラメータを中心として，その値を十分大きくしたときの振る舞いを調べることを漸近的解析という．例えば，$f(n) = 6n^3 + 5n^2 + 4n + 10$ は 4 つの項をもつが，n を十分大きくしたとき，$f(n)$ において $6n^3$ の項がもっとも大きく影響している．このとき，n^3 の係数 6 を無視し，f は漸近的には n^3 以下であるという．漸近記法では，$f(n) = O(n^3)$ と書く．

より正確な定義を与える．二つの関数 $f, g : \mathbb{N} \to \mathbb{R}$ に対して，ある正整数 n_0 と c が存在し，$n \geq n_0$ であるすべての n に対して $f(n) \leq cg(n)$ であるとき，$f(n) = \mathrm{O}(g(n))$ と書く．また，$g(n) = \mathrm{O}(f(n))$ のとき，$f(n) = \Omega(g(n))$ と書く．さらに，$f(n) = \mathrm{O}(g(n))$ かつ $g(n) = \mathrm{O}(f(n))$ であるとき，$f(n) = \Theta(g(n))$ と書く．

他の記法として，f が g に比べ，漸近的に真に小さいとき，$f(n) = \mathrm{o}(g(n))$ と書く．正確に定義すると，任意の正実数 ϵ に対し，ある正整数 n_0 が存在し，$n \geq n_0$ であるすべての n に対して $f(n) < \epsilon g(n)$ であるとき，$f(n) = \mathrm{o}(g(n))$ と書く．

記法	定義	解釈
$f(n) = \mathrm{O}(g(n))$	$\exists n_0, c, \forall n \geq n_0, f(n) \leq cg(n).$	f は g の定数倍で上から抑えられる．
$f(n) = \Omega(g(n))$	$\exists n_0, c, \forall n > n_0, g(n) \leq cf(n).$	f は g の定数倍で下から抑えられる．
$f(n) = \Theta(g(n))$	$f(n) = \mathrm{O}(g(n))$ かつ $f(n) = \Omega(g(n))$	f は g と定数倍の範囲で同じ大きさである．
$f(n) = \mathrm{o}(g(n))$	$\forall \epsilon > 0, \exists n_0, \forall n > n_0, f(n) < \epsilon g(n).$	f は g より真に小さい大きさである．
$f(n) \sim g(n)$	$f(n) = (1 + \mathrm{o}(1))g(n)$	f は g と主係数を同じとする大きさである．

$f(n) = \mathrm{O}(n)$ のとき，ある定数 c によって $f(n)$ は cn で上から抑えられることを意味する．同様の考え方により，O が指数部に表れることもある．つまり，$f(n) = 2^{O(n)}$ とは，ある定数 c によって $f(n)$ は 2^{cn} で上から抑えられることを意味する．

また，$f(n) = \log_2 n$ のとき，対数の底を任意の正定数 b に変えたとしても，$\log_b n = \log_2 n / \log_2 b$ であり，大きさは定数倍程度しか変わらない．したがって，底を無視して，$f(n) = \mathrm{O}(\log n)$ と書く．

例 1

1. $f_1(n) = 5n^3 + 7n^2 + 100n + 1000$ のとき，$f_1(n) = \mathrm{O}(n^3), f_1(n) = \mathrm{O}(n^4), f_1(n) = \Omega(n^2), f_1(n) = \Theta(n^3), f_1(n) = \mathrm{o}(n^4)$ は正しい．しかし，$f_1(n) = \mathrm{O}(n^2), f_1(n) = \Omega(n^4), f_1(n) = \mathrm{o}(n^3)$ は間違い．
2. $n\sqrt{n} = \mathrm{o}(n^2)$.
3. $n = \mathrm{o}(n \log n)$.
4. $100 = \mathrm{O}(1)$.

2 Gilbert-Varshamov 限界

Gilbert-Varshamov 限界は，漸近的によい符号が存在することを示している．

定義 2 (エントロピー関数) 実数 $0 \leq x \leq 1$ に対し，エントロピー関数 $H(x)$ は

$$H(x) = x \log_2 \frac{1}{x} + (1-x) \log_2 \frac{1}{1-x}.$$

定理 3 (Gilbert-Varshamov 限界) 実数 $0 \leq \delta \leq 1/2$ に対して，相対最小距離 δ，レート $R \geq 1 - H(\delta)$ の二元符号族が存在する．

以下では，上記定理に対して異なる証明を与える．証明を与える前に，証明で利用する補題を示す．

2.1 エントロピー関数と Hamming 球の体積

定義 4 (Hamming 球) $x \in \{0,1\}^n$ と実数 r に対して，x を中心とした半径 r の Hamming 球とは，

$$B(x,r) = \{y \in \{0,1\}^n : d(x,y) \leq r\}.$$

Hamming 球の体積は，x に依存しないため， $\mathrm{Vol}(n,r) = |B(x,r)|$ と表す．すると，

$$\mathrm{Vol}(n,r) = \sum_{j=0}^{r} \binom{n}{j}.$$

補題 5 十分大きな n，$0 \leq p \leq 1/2$ に対して，

$$2^{(H(p)-o(1))n} \leq \mathrm{Vol}(n,pn) \leq 2^{H(p)n}.$$

証明: まず上界を示す．

$$\begin{aligned}
\frac{\mathrm{Vol}(n,pn)}{2^{H(p)n}} &= \frac{\sum_{j=0}^{pn} \binom{n}{j}}{p^{-pn}(1-p)^{-(1-p)n}} \\
&= \sum_{j=0}^{pn} \binom{n}{j} p^{pn} (1-p)^{(1-p)n} \\
&= \sum_{j=0}^{pn} \binom{n}{j} (1-p)^n \left(\frac{p}{1-p}\right)^{pn}.
\end{aligned}$$

ここで，$p \leq 1/2$ であり， $p/(1-p) \leq p$ であるので，上式は

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

で抑えられる．二項定理より，上式は

$$\sum_{j=0}^{n} \binom{n}{j} (1-p)^{n-j} p^j = 1$$

で抑えられる．したがって，$\mathrm{Vol}(n, pn) \leq 2^{H(p)n}$ が導かれる．

次に下界を示す．Stirling の公式

$$m! = \sqrt{2\pi m}\left(\frac{m}{e}\right)^m (1 + \mathrm{o}(1)).$$

を使うと，

$$\begin{aligned}
\binom{n}{pn} &= \frac{n!}{(pn)!((1-p)n)!} \\
&\geq \frac{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n}{\sqrt{2\pi pn}\left(\frac{pn}{e}\right)^{pn}(1+\mathrm{o}(1)) \cdot \sqrt{2\pi(1-p)n}\left(\frac{(1-p)n}{e}\right)^{(1-p)n}(1+\mathrm{o}(1))} \\
&\geq \left(\frac{1}{p}\right)^{pn}\left(\frac{1}{1-p}\right)^{(1-p)n}\exp(-o(n)) \\
&= 2^{H(p)n-o(n)}.
\end{aligned}$$

したがって，

$$\mathrm{Vol}(n, pn) \geq \binom{n}{pn} \geq 2^{H(p)n-o(n)}.$$

■

2.2 貪欲法による符号の構成

Gilbert は最小距離 d の符号を構成する方法として，以下の方法を考えた．

1. 初期化: $S \leftarrow \{0,1\}^n, C \leftarrow \emptyset$.
2. $S = \emptyset$ となるまで以下を繰り返す:
   (a) $x \in S$ を選び，x を C に加える．
   (b) S から $B(x, d-1)$ を削除．

補題 6 上記の方法で得られる符号 C は，次式を満たす．

$$|C| \geq \frac{2^n}{\mathrm{Vol}(n, d-1)} = \frac{2^n}{\sum_{j=0}^{d-1}\binom{n}{j}}.$$

証明: ステップ 2 において，$S = \emptyset$ となったとする．このとき，C に含まれる符号語を中心とした半径 $d-1$ の Hamming 球によって，$\{0,1\}^n$ はすべて覆われている．なぜならば，もしそうでないとすると，覆われていない点は C に含まれる符号語と Hamming 距離が d であり，ステップ 2 が終了していないことになる．したがって，得られた C は以下を満たす．

$$|C| \cdot \mathrm{Vol}(n, d-1) \geq 2^n.$$

■

Gilbert-Varshamov 限界を証明する．相対最小距離 $0 \leq \delta \leq 1/2$ に対して，$d = \delta n$ として上記補題を適用する．すると，レート R は

$$\begin{aligned} R &= \frac{\log_2 |C|}{n} \\ &\geq \frac{n - \log_2 \mathrm{Vol}(n, \delta n - 1)}{n} \\ &\geq \frac{n - H(\delta - 1/n)n}{n} \\ &\geq 1 - H(\delta). \end{aligned}$$

上記の不等式の導出では，補題 5 とエントロピー関数 $H(x)$ の $0 \leq x \leq 1/2$ における単調増加性を利用している．

補足 7 Varshamov は上記と同様の貪欲法が，線形符号に対しても可能であることを示した．ただし，Varshamov の方法で得られる $(n, k, d)_2$ 線形符号 C は

$$k \geq n - \lfloor \log_2 (\mathrm{Vol}(n-1, d-2) - 1) \rfloor$$

であり，得られた符号のレートは Gilbert の方法よりもわずかに小さい．ただし，漸近的なレートは Gilbert-Varshamov 限界に一致する．

3 ランダム線形符号

ランダムに生成した線形符号は高い確率で Gilbert-Varshamov 限界を満たすことを示す．ランダム線形符号とは，$k \times n$ 行列 G の各エントリーを $\{0, 1\}$ から独立に一様に選び，その G を生成行列とする線形符号である．

定理 8 任意の $0 \leq \delta \leq 1, \epsilon > 0$, 十分大きな $n, k = \lceil (1 - H(\delta) - \epsilon)n \rceil$ に対して以下が成り立つ．$G \in \{0, 1\}^{k \times n}$ をランダムに選んだとき，G を生成行列とする線形符号は，相対最小距離が δ 以上，レートが $1 - H(\delta) - \epsilon$ 以上である確率が $1 - e^{-\Omega(n)}$ 以上である．

証明: まず，レートについて証明する．これは，G がフルランクであることを示せば十分である．G の i 行目の行が，最初の $(i-1)$ 行によって張られる空間に含まれる確率は，$2^{i-1}/2^n$ 以下である．和集合上界より，G のランクが k である確率は，$1 - \frac{k}{2^{n-k}} \geq 1 - e^{-\Omega(n)}$.

次に，最小距離について証明する．非零である $x \in \{0, 1\}^k$ に対して，xG は $\{0, 1\}^n$ から一様ランダムに選んだベクトルとなる．したがって，$\mathrm{wt}(xG) \leq \delta n$ である確率は，補題 5 を使うと，

$$\frac{\mathrm{Vol}(n, \delta n)}{2^n} \leq 2^{(H(\delta)-1)n}$$

以下である．すべての非零符号語の Hamming 重みが δn 以下である確率は，和集合上界を用いると，

$$2^k \cdot 2^{(H(\delta)-1)n} \leq 2^{(1-H(\delta)-\epsilon)n+1} \cdot 2^{(H(\delta)-1)n} = 2^{1-\epsilon n} \leq e^{-\Omega(n)}$$

以下である．したがって，相対最小距離が δ 以上である確率は $1 - e^{-\Omega(n)}$ 以上である．■