Gilbert-Varshamov Bound

Mitsuru Takigahira

TL;DR

- 良い誤り訂正能力を維持しながら、伝達速度 $R = \frac{1}{n}\log_q M$ を最大化するために、与えられた q, n 及び t (または同値な d) に対して、可能な限り大きい値 $M = \mid C \mid$ となる符号を探すことを目的とする。
- q, n, d が与えられたときの最大の符号語数について上界と下界を求め、伝送速度 R の下界をを求めていく。

符号語数の上界

定義

$A_q(n,d)$ を任意の符号長 n、最小距離 d の q 元符号の符号語数の最大値と置く。ここで $d \leq n$ である。

ハミングの球充填限界式 (定理 6.15) から $A_q(n,d)$ の上界は次のように与えられる。

$$A_q(n,d)\left(1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{t}(q-1)^t\right)\leq q^n$$

$t=\lfloor (d-1)/2 \rfloor$ (定理 6.10)

例 6.20

$q = 2$ と $d = 3$ の場合、$t = 1$ で、例 6.16 で見たように、$A_2(n, 3) \leq \lfloor 2^n/(n+1) \rfloor$
よって、$n = 3, 4, 5, 6, 7, \ldots$ に対して、$A_2(n, 3) = 2, 3, 5, 9, 16, \ldots$

練習 6.9

例 6.20 で $A_2(n, 3)$ の上界を求めたように、$A_3(n, 3)$ の上界を求めよ。ハミングの球充填限界式は $A_2(n, 4)$ と $A_2(n, 5)$ に関してどうなるか？

定理 6.21

似たような議論から、与えられた q, n そして d に対して、与えられた最小の符号語数を持つ符号が存在することを示すことによって、$A_q(n, d)$ の下界が得られる。これが Gilbert-Varshamov 限界である。

定理 6.21

$q \geq 2$ かつ $n \geq d \geq 1$ のとき

$$A_q(n,d)\left(1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{d-1}(q-1)^{d-1}\right) \geq q^n$$

証明: 定理 6.21

与えられた q, n 及び d を満たす全ての符号に関して、C を最大の符号語数を持つ符号と置く。つまり、$M = \mid C \mid = A_q(n, d)$ である。$\mathbf{u} \in C$ なる全ての球

$$S_{d-1}(\mathbf{u}) = \{\mathbf{v} \in \mathcal{V} \mid d(\mathbf{u}, \mathbf{v}) \leq d - 1\}$$

は、$\mathcal{V}$ を覆う。なぜなら、もし $\mathbf{v} \in \mathcal{V}$ がどの $S_{d-1}(\mathbf{u})$ にも含まれないとすると、任意の $\mathbf{u} \in C$ に対して $d(\mathbf{u}, \mathbf{v}) \geq d$ で、符号 $C' = C \cup \{\mathbf{v}\}$ は同じ q, n 及び d の値を持つが、これは C の選び方に反するからである。(6.6) を証明した議論によって、それぞれ M 個の球 $S_{d-1}(\mathbf{u})$ は $\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i$ 個のベクトルを含んでいる。以上から、これらの球は全ての $\mathcal{V}$ 上 q^n 個の全てのベクトルを含んでいるので、上式を満たす。

例 6.22

例 6.22

$q=2$ と $d=3$ をとると ($\therefore t=1$)、定理 6.21 は全ての $n\geq 3$ に対して、

$$A_2(n,3)\left(1+n+\frac{n(n-1)}{2}\right)\geq 2^n$$

よって $A_2(n,3)\geq 2^{n+1}/(n^2+n+2)$ である。$A_q(n,d)$ は整数より

$$A_2(n,3)\geq \lceil 2^{n+1}/(n^2+n+2)\rceil$$

$n=3,4,5,6,7,\ldots$ に対して、$A_2(n,3)\geq 2,2,2,3,5$

- 例 6.20 で、上界と下界を比べる場合、$A_2(3,3)=2$ である。

  ex 2 元反復符号 $\mathcal{R}_3$ はこの境界を満たす。
- $n=4$ のとき、$2\leq A_2(4,3)\leq 3$ で、$A_2(4,3)=2$ or 3 である。

練習問題

練習 6.10

$A_2(4,3) = 2$ を示し、この境界に達する符号を示せ。

練習 6.11

$A_3(n,3)$ の下界を求めよ。

$A_q(n,d)$ の正確な値

- 多くの q, n と d に対して、$A_q(n,d)$ の上界と下界には大きな差がある。
  - この正確な値を求めるのは難しい
  - 多くの場合この値はわからない。
- 場合によっては特殊な符号がこの値の存在を教えてくれる。
  - $q = 2, d = 3$ で $n = 7$ のとき、ハミング符号 $\mathcal{H}_7$ は定理 6.15 から上界 $M \leq 16$ に達する。よって $A_2(7,3) = 16$ である。
- §7.4 ではより一般的に、n が $2^c - 1$ の形をしているとき、$A_2(n,3)$ は上界 2^{n-c} に達することを確認する。

2 元符号の伝送速度

2 元符号の場合、定理 6.21 は以下の形になる。

$$A_2(n,d)\left(1+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{d-1}\right)\geq 2^n$$

今、練習 5.7 から $Q<\frac{1}{2}$ のとき

$$\sum_{i\leq nQ}\binom{n}{i}\leq 2^{nH_2(Q)}$$

よって、$d\leq\lfloor n/2\rfloor$ に対して、

$$\log_2 A_2(n,d)\geq n\left(1-H_2\left(\frac{d-1}{n}\right)\right)$$

2 元符号の伝送速度

2 元符号は伝送速度 $R = \frac{1}{n}\log_2 M$ なので、これは $d \leq \lfloor n/2 \rfloor$ のとき符号長が n、最小距離が d で、伝送速度が

$$R \geq 1 - H_2(\frac{d-1}{n})$$

なるような符号が存在することを示している。
これは定理 6.10 によって $t = \lfloor (d-1)/2 \rfloor$ の下
§6.4 で証明したハミングの漸近的上界

$$R \leq 1 - H_2(\frac{t}{n})$$

と比べることが出来る。
図 6.6 は R のこれら 2 つの境界によって定義される領域を表している。