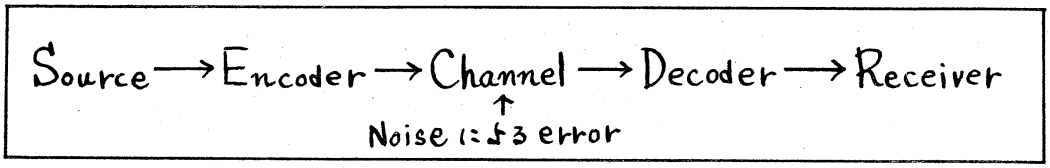
数理解析研究所講究録
第82巻 1970年 1-11

Algebraic Coding Theory
における二，三の話題

海上保安大　福田常次郎

1. Error correcting codes



有限体 $GF(q=p^{\Delta})$ 上の n 次元ベクトル空間 V_n の一つの部分集合 C を長さ n のブロック符号系という。 $q=2$ の場合が2元符号，$q>2$ の場合が多元符号と呼ばれている。 以下簡単のため，主に対称2元符号について考える。

代数的符号化，すなわち，雑音のある離散的通信路上の符号化の基本問題は，符号系 C の中の一つのベクトル(code word)が送信されたとき，仮に途中でerrorsが起ったとしても，受信されたベクトルから送られた元の code word を推定できる機構を持つように C を選定することである。

その機構とは次のようなものである。

$\forall x_i, x_j \in C$ に対して， $x_i \neq x_j \Longrightarrow R_{x_i} \cap R_{x_j} = \phi$ であるような V_n の部分集合 R_{x_i}, R_{x_j} を定め，x_i に対する受信ベクトルを $\overline{x_i}$ とするとき，$\overline{x_i} \in R_{x_i}$ ならば送信された word は x_i であると推定する。 この部分集合 R_{x_i} を x_i に対する detection region という。 detection region の選定には次の二つの立場がある。

(1) Minimum distance codes

$\forall x_i = (x_{i1}, x_{i2}, \cdots, x_{in})$, $x_j = (x_{j1}, x_{j2}, \cdots, x_{jn}) \in C$ に対して $d(x_i, x_j) = \sum_{l=1}^{n} (x_{il} - x_{jl})$ を x_i と x_j との間の Hamming distance といい， x_i, x_j を C の中で動かしたときの距離の最小値 d を C の minimum distance という。

この場合，x に対する detection region として

$$R_x = \left\{ y \in V_n \mid d(x, y) \leqq \left[\frac{d-1}{2}\right]^{*)} \right\}$$

すなわち，Hamming distance criterion の下で x に最も近いベクトル(の集合)が選ばれる訳で， maximum likelihood decoding と呼ばれている。

(2) Linear (Group) codes

符号系 C が V_n の k 次元線形部分空間であるとき，Linear code または group code といい， (n, k) code と書く。

linear code に対する detection region 決定には次のような

---

*) $[t]$ は Gauss 記号で t を越えない最大の整数を表わす。

Standard array が利用される。

C を加群 V_n の部分加群とみて

$$x_0=0,\ x_1,\ \cdots,\ x_i,\ \cdots,\ x_{2^k-1} \longleftrightarrow C$$

$$g_1,\ g_1+x_1,\ \cdots,\ g_1+x_i,\ \cdots,\ g_1+x_{2^k-1} \longleftrightarrow g_1+C$$

$$g_2,\ g_2+x_1,\ \cdots,\ g_2+x_i,\ \cdots,\ g_2+x_{2^k-1} \longleftrightarrow g_2+C$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

を V_n の C による剰余類表とする。 coset leader g_j がその coset 中 minimum weight *) のものとして選ばれているとき，この剰余類表は standard array と呼ばれる。

このとき，code word x に対する detection region として

$R_x=\{x,\ g_1+x,\ g_2+x,\ \cdots\}$ を採用する。

minimum distance codes では detection region の選定原理が与えられているだけで，具体的な複号化方式は示されておらず，又，linear codes に対する standard array による複号化表は n, k が大きいときは実用的でない。 これらの混合型とでもいうべき立場に立つのが次のような codes である。

(3) Cyclic linear codes , Majority decodable codes

一つの linear code C は，

---

*) $x_i=(x_{i1}, x_{i2}, \cdots, x_{in})$ とするとき， $w(x_i)=\sum_{l=1}^{n} x_{il}$ をベクトル x_i の Hamming weight という。

$x=(x_1, x_2, \cdots, x_n) \in C \Longrightarrow y=(x_n, x_1, x_2, \cdots, x_{n-1}) \in C$

という条件を充すとき cyclic code と呼ばれる。この条件は V_n を x^n-1 を法とする GF(2) 上の多項式環と考えたとき，C が一つの ideal をなすということと同値である。しかもこの場合 C は単項 ideal であることからその構造は生成多項式によって完全に規定され，複号化は standard array 利用に比べると極めて簡単になる。その代表的 code として，Bose-Chaudhuri-Hocquenghem codes や修正 Reed-Muller codes などがある。

また cyclic codes とは別に，多数決論理によって比較的簡単に複号化可能な majority decodable codes の研究も進んでいる。代表的な例は Reed Muller codes や Finite geometry codes などである。

これら一連の有名な codes は単に複号化が簡単であるばかりでなく，minimum distance 或いはその下限が判っており多重誤り訂正が可能である[3]。

2. Maximal codes

code length n と minimum distance d が与えられたときこれら2つの parameters を持つ codes の中で words の個数が最大であるものを求めるという問題は一般に未解決である。

(1)　$A(n, d)$ について

n, d を parameters とする maximal code の words の個数を $A(n, d)$ で表わす。$A(n, d)$ については種々の bounds が与えられているが，その正確な値はほとんど知られていない[2]。

実験計画法における対称釣合型不完備ブロック計画(SBIBD)の存在問題とも関係する有名な問題の一つが次の予想である。

[Conjecture]　すべての正整数 t に対して

(i)　$A(4t-2, 2t) = 2t$

(ii)　$A(4t-1, 2t) = 4t$

(iii)　$A(4t, 2t) = 8t$

} が成立するであろう。

この予想には次の諸定理が関係している。

[定理] (Plotkin, 1951)

(1) (i)　$A(4t-2, 2t) \leqq 2t$

(ii)　$A(4t-1, 2t) \leqq 4t$

(iii)　$A(4t, 2t) \leqq 8t$

} がすべての正整数 t に対して成立する。

(2)　$A(4t, 2t) = 8t \Longrightarrow$ (i) と (ii) で等号が成立する

(3)　$4t-1$ が素数ならば　$A(4t, 2t) = 8t$。

[定理] (Bose and Shrikhande, 1959)

次の4命題は同等である。

(a)　$A(4t, 2t) = 8t$

(b) $A(4t-1, 2t) = 4t$

(c) $v = k = 4t-1$, $r^* = k^* = 2t-1$, $\lambda = t-1$ を parameters とする SBIBD が存在する。

(d) order $4t$ の Hadamard 行列 H_{4t} が存在する。

[定理] (Brauer, 1953 及び Stanton and Sprott, 1958)

Hadamard 行列 H_k が存在するための十分条件は次の通りである。

(i) $k = 2^k$

(ii) $k = p^k + 1 \equiv 0 \pmod 4$; p は prime

(iii) $k = k_1(p^k+1)$; $k_1 \geq 2$ は Hadamard 行列の order

(iv) $k = k^*(k^*-1)$; k^* は (i) と (ii) の積

(v) $k = 172$

(vi) $k = k^*(k^*+3)$; k^* と k^*+4 は共に (i) と (ii) の積

(vii) $k = k_1 k_2 (p^k+1) p^k$; $k_1 \geq 2$, $k_2 \geq 2$ は共に Hadamard 行列の order

(viii) $k = k_1 k_2 s(s+3)$; $k_1 \geq 2$, $k_2 \geq 2$ は共に Hadamard 行列の order

s, $s+4$ は共に p^k+1 の形

(ix) $k = (q+1)^2$; q と $q+2$ は共に prime または prime power

(x) k は (i) ～ (ix) の積。

(註) M. Hall ; Combinatorial Theory, Ginn and Company 1967 によると, 上記の他 $k=92$, $k=116$ の場合も存在する。

(2) $B(n,d)$ について

n, d を parameters とする maximal linear code の words の個数を $B(n,d)$ で表わす。

$d=1$, $d=2$ のときは自明で $B(n,1)=2^n$, $B(n,2)=2^{n-1}$ である。

$d=3$ の場合は次の2つの定理によって完全に解決されている。

[定理] (Hamming, 1950)

$n=2^m-1$ ならば $B(n,3)=A(n,3)=2^{n-m}$

[定理] (Shapiro and Slotnick, 1959)

$n\neq 2^m-1$ ならば $2B(n,3)=B(n+1,3)$

$d=4$ の場合も, Hamming の定理: $B(n-1,2k-1)=B(n,2k)$ を使うと, $d=3$ の結果を利用することにより, すべての n に対して $B(n,4)$ の値を求めることができる。

$d>4$ の場合については一般に未解決である[2]。この問題に対しては次の2通りのアプローチが考えられる。

(1°) Generator matrix によるアプローチ

問題を次のように formulate する

「k, d が与えられたとき, d を minimum distance, k を information symbols の個数とする linear code の code length n の最小値はいくらか?」

nに対する下限は次の定理により与えられている。

[定理] (Griesmer , 1960) [1]

k, d が与えられたとき， 一つの (n, k) code が minimum distance d を持つならば

$$n \geqq d + d_1 + d_2 + \cdots + d_{k-1}$$

ここに $d_1 = \left[\frac{d+1}{2}\right]$, $d_{i+1} = \left[\frac{d_i+1}{2}\right]$ $(i = 1, 2, \cdots, k-2)$.

さて， G を一つの (n, k) code の generator matrix とすると，G の列ベクトルは GF(2) 上の $(k-1)$次元射影空間 PG$(k-1, 2)$ の点の座標表現とみなすことができる。 よって G はこの射影空間の点の全体から成る $k \times (2^k - 1)$ 行列 G_0 の部分集合である。

d を指定したとき， G_0 の部分集合である generator matrix G はどのような性質を有しているであろうか？

これに対する一つの解答が次の定理である。

[定理] (Solomon and Stiffler , 1965) [4]

(i) $1 \leqq l_i \leqq k-1$, $\sum_{i=1}^{s} l_i \leqq k$ を充す s 個の正整数 $\{l_i\}$ に対して， 互に素な s 個の (l_i-1)-flats を除いて得られる行列 G を generator matrix とする $\left(2^k - 1 - \sum_{i=1}^{s}(2^{l_i}-1),\ k\right)$ code は minimum distance $d = 2^{k-1} - \sum_{i=1}^{s} 2^{l_i - 1}$ を持つ。

(ii) (i)において $l_i \neq l_j$ $(i \neq j)$ ならば， この code は code length n が Griesmer bound theorem における下限を

attainしているという意味でoptimalである。つまり，maximal codeである。

(例1) $\delta=1$のときがMacDonald codeである。

特に $\ell=k-1$ とすると $B(2^{k-1}, 2^{k-2})=2^k$ を得る。これは $A(4t, 2t)=8t$ に対応しており，$k=4t=2^{k-1}$の場合はMacDonald code或いは1st order Reed-Muller codeなどのlinear codeで，このparametersを持つmaximal codeが得られることを示している。

(例2) $\delta=1$, $\ell=1$ とすると $B(2^k-2, 2^{k-1}-1)=2^k$

これからHammingの定理 $B(n-1, 2k-1)=B(n, 2k)$ を使って $B(2^k-1, 2^{k-1})=2^k$ を得る。これは $A(4t-1, 2t)=4t$ に対応しており，$k=4t=2^k$ の場合はfull matrix G_0 をgenerator matrixとするequidistant linear codeでmaximal codeが得られることを示している。

(註) Hamming $(2^m-1, 2^m-1-m)$ codeはmaximal linear codeであるが，code length $n=2^m-1$ がGriesmer lower boundをattainするのは $m=3$ の場合だけで，$m>3$ ならばこの下限より大きくなる。

(2) Parity check matrixによるアプローチ

n_0 をcode length，r をredundancy，d_0 をminimum

distance とする一つの maximal code C_0 が存在したとする。この code の parity check matrix H_0 から列ベクトルを適当に落すことによって code length n_0 を減らす一方，minimum distance d_0 を大きくして行く立場である。

(例3)　minimum distance 4 の modified Hamming code.

Hamming $(2^r-1,\ 2^r-1-r)$ code の parity check matrix H_0 の列ベクトルを $PG(r-1,2)$ の点とみなすと次の Lemma が成り立つ。

[Lemma]　H_0 の列ベクトルの一つの部分集合を H とし，H を parity check matrix とする code C が minimum distance 4 を持つための必要十分条件は，H が $PG(r-1,2)$ の直線を一本も含まないことである。

この条件は，一つの超平面 Π を H_0 から除いた部分集合を H として選ぶことにより達成される。　この場合

$n=2^r-1-(2^{r-1}-1)=2^{r-1}$,　$k=2^{r-1}-r$,　$d=4$

(具体例)　$r=4$ の場合

$$H_0=\left[\begin{array}{ccccccccccc:cccc}
1&0&1&1&1&0&0&0&1&1&1&1&0&0&0\\
1&1&0&1&1&0&1&1&0&0&1&0&1&0&0\\
1&1&1&0&1&1&0&1&0&1&0&0&0&1&0\\
1&1&1&1&0&1&1&0&1&0&0&0&0&0&1
\end{array}\right]$$

$$H=\left[\begin{array}{ccc:cccc}
0&1&1&1&1&0&0&0\\
1&0&1&1&0&1&0&0\\
1&1&0&1&0&0&1&0\\
1&1&1&0&0&0&0&1
\end{array}\right]$$

$$\Pi=\left[\begin{array}{ccccccc}
1&1&1&0&0&0&1\\
1&0&0&1&1&0&1\\
0&1&0&1&0&1&1\\
0&0&1&0&1&1&1
\end{array}\right]$$

参考文献

[1] Griesmer,J.H.(1960): A bound for error correcting codes. IBM J.Res. Develop. 4, No.5.

[2] Joshi,D.D.(1963): Coding theory(Summer course for statisticians). Research and Training School, Indian Statist. Inst.

[3] Peterson,W.W.(1961): Error correcting codes. MIT Press and Wiley, New York.

[4] Solomon,G.and Stiffler,J.J.(1965): Algebraically punctured cyclic codes. Information and Control 8, 170-179.