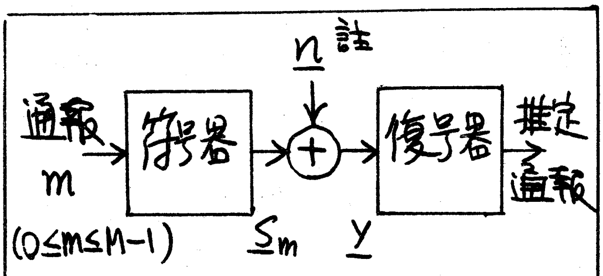
数理解析研究所講究録
第 82 巻 1970 年 31-40

巡回変換群信号集合のパラメタの最適化

東京大学宇宙航研　　伊藤紘二

§1. まえがき

n-tuple空間で，ベクトルを運動させて得られる信号集合を図1の，加算的ガウス雑音がある伝送路を通してのブロック符号通信に用いる時，この運動の集合が，一つの群をなしていることが，信号集合が対称性——どの信号が送られても最尤法による受信誤判定率は等しい——を有する為の必要十分条件である。[1] この種の信号集合の中で最も簡単なのは，運動が巡回群をなす場合で，その標準形直交表現によってつくられたものを，ここでは巡回変換群信号集合—— Cyclic Group Signal set, 略してCGS ——と



各ベクトルは n-tuple. $\underline{n}$ の各成分は独立な分散 $N_0/2$ のガウス分布をする.

図1. ブロック符号通信

註：小文字の下の＿はそれがベクトルであることを示す。

称し，以下その簡単な紹介をし，パラメタの最適化の問題の取扱いにおいて得られたいくつかの結果を記す。

§2. CGSを用いる通信方式

CGS $\{\underline{s}_m\}$ 註 は結局，

$$\left.\begin{array}{ll} \underline{s}_m = {}^t\left(s_{11}^{(m)}, s_{12}^{(m)}, s_{21}^{(m)}, s_{22}^{(m)}, \cdots, s_{N1}^{(m)}, s_{N2}^{(m)}\right)^{\text{註}} & \\ s_{n1}^{(m)} = a_n \cos\left(\frac{2\pi}{M} m k_n\right) & (k_n\text{は整数}) \\ s_{n2}^{(m)} = a_n \sin\left(\frac{2\pi}{M} m k_n\right) & (0 \le m \le M-1) \end{array}\right\} \quad (1)$$

という形になり，信号次元数は2Nである。

さて，このCGSは，そのパラメタ $\{a_n\}$，$\{k_n\}$ をうまく選べば，情報伝送速度 $R = \log_2 M/2N$ と，伝送路信号対雑音比 $A = \sum_{n=1}^{N} a_n^2/(N_0 \cdot N)$ を与えた時，最尤法による誤判定率 P_e が，

$$P_e \le e^{-2NE_Q(R, A)}, \quad R < {}^{\exists}C_Q(A) \qquad (2)$$

の形の上界を有することが導びかれている[3]。ここに $E_Q(R, A)$ は，Mの含む最小の約数 $Q(\ge 2)$ に依存するが，Rに関して単調減少である。また，CGSは，その構造の特性から，復号法にある工夫を施すことができる[2]。この様に，CGSの有効性は確かめられるのであるが，実際に a_n，k_n を選んで，実用し得る信号を求める必要がある。次節以降はこの問

註：$\{x_n\}$ は，$x_1, x_2, \cdots$ の集合。${}^t\underline{x}$ は $\underline{x}$ の転置。

題を扱う。

§3. CGSのパラメタの最適化.

CGSは，対称性を有する等エネルギ信号集合であるから，信号間の正規化された相互相関（例えば第0信号を基準にして）$\rho_{0\ell}$（$1 \leq \ell \leq M-1$）の最大値 ρ_{max} の小さい程良い信号集合であると考えられる。ここで，(1)から，

$$\rho_{0\ell} = \sum_{n=1}^{N} X_n \cos \frac{2\pi}{M} k_n \ell \qquad (3)$$

$$\left(X_n = a_n^2 \Big/ \sum_{n=1}^{N} a_n^2 \right)$$

であるから，

$$\left.\begin{aligned} \rho_{max} &\geq \sum_{n=1}^{N} X_n \cos \left(\frac{2\pi}{M} k_n m \right) \quad 1 \leq m \leq M_h \\ 1 &= \sum_{n=1}^{N} X_n \qquad X_n \geq 0 \end{aligned}\right\} \quad (4)$$

という条件の下に ρ_{max} を成可く小さくする様な $\{X_n\}$, $\{k_n\}$ を求めればよい。ここで，$M_h = [M/2]$ であり，(4)の上式で $m > M_h$ の場合を省いてあるのは，$\cos\left(\frac{2\pi}{M}(M-m)k_n\right) = \cos\left(\frac{2\pi}{M} m k_n\right)$ が成立するからである。

さて，最適解を求めるには，

a）$\{k_m\}$ を与える。

b）与えられた $\{k_m\}$ に対して（4）の条件で ρ_{max} を最小

にする $\{X_n\}$ を求める。これは線型計画法の手法によって求めることができる。そして,

互いに一致しない解を与える $\{k_n\}$ のあらゆるものに対して a), b) を実行し,こうして得られた各 $\{k_n\}$ に対する ρ_{max} の最小値の中で最も小さい値を与える $\{k_n\}$ が最適である。之に対応して最適な $\{X_n = a_n^2/\sum a_n^2\}$ が求まっている。

ところで,ここに,上記の如き $\{k_n\}$ を次々に供給する能率のよい方法が必要である。まず信号次元を無駄に使わぬ為,

i) k_n の値としては 0 は採用しない。

ii) $\{k_n\}$ の元のどの二つ k_n, $k_{n'}$ についても,$k_{n'} \equiv \pm k_n \bmod M$ が成立しない様にすること。何故なら,このような対があると,その ρ_{0l} への寄与は,

$$X_n \cos\frac{2\pi}{M}k_n l + X_{n'}\cos\frac{2\pi}{M}(\pm k_n + qM)l = (X_n + X_{n'})\cos\frac{2\pi}{M}k_n l$$

であって,一つの次元にまとめ得るからである。

更に,$\{k_n\}$ の候補は,全く同じ $\{\rho_{0l}\}$ を与える一従がって同じ最適解を与える一もの同志を一まとめにしたいくつかのグループに分けられる。事実 $\{k_n\}$ の2つの候補 $\{k_n^{(1)}\}$, と $\{k_n^{(2)}\}$ とがあったとき,

iii) M とは互いに素である整数 μ が存在して,

$$\{k_n^{(2)}\} = \{\mu k_n^{(1)}\} \bmod M$$

が成立するとき,この2つの候補は同じ $\{\rho_{0l}\}$ を与えるこ

とが容易に示される（∵通報番号mを$m\mu$に変換して一対一対応がつく）。

我々は，i），ii），iii）に注意しつつ$\{k_n\}$の候補を供給したい。これは，Mが素数のとき，次節に示す方法により能率よく実行することができる。

§4. $\{k_n\}$の供給，—Mが素数の場合.

前節 i）から，k_nとしては0は採用しないから，k_nをM元のガロア体の原始根rによって

$$k_n = r^{s_n} \mod M \qquad 1 \leq n \leq N$$

のように表現し，$\{k_n\}$を考える替りに$\{s_n\}$を扱うことができる。さて，$M_h = (M-1)/2$であるから，$r^{M_h} \equiv -1 \mod M$となり，ii）を考慮すれば，s_nとしては$0, 1, 2, \cdots \cdots M_h - 1$の中から互いに異なるものを選べばよい。順序は自由なので$s_1 < s_2 < \cdots < s_N$とする。更に iii）を考慮すれば，2つの候補$\{s_n^{(1)}\}$，$\{s_n^{(2)}\}$に対し，ある整数dが存在して

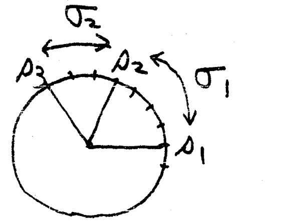
$$\{s_n^{(2)}\} = \{s_n^{(1)} + d\} \quad \mod M_h$$

ならば$\{s_n^{(1)}\}$と$\{s_n^{(2)}\}$とは同等—同じ$\{\rho_{0\ell}\}$を与える—である。そこで，s_nとs_{n-1}との差を表わす系列

$$(\sigma_1, \sigma_2, \cdots, \sigma_N) \qquad 1 \leq \sigma_i \leq M_h \ , \quad \sum_{i=1}^{N} \sigma_i = M_h$$

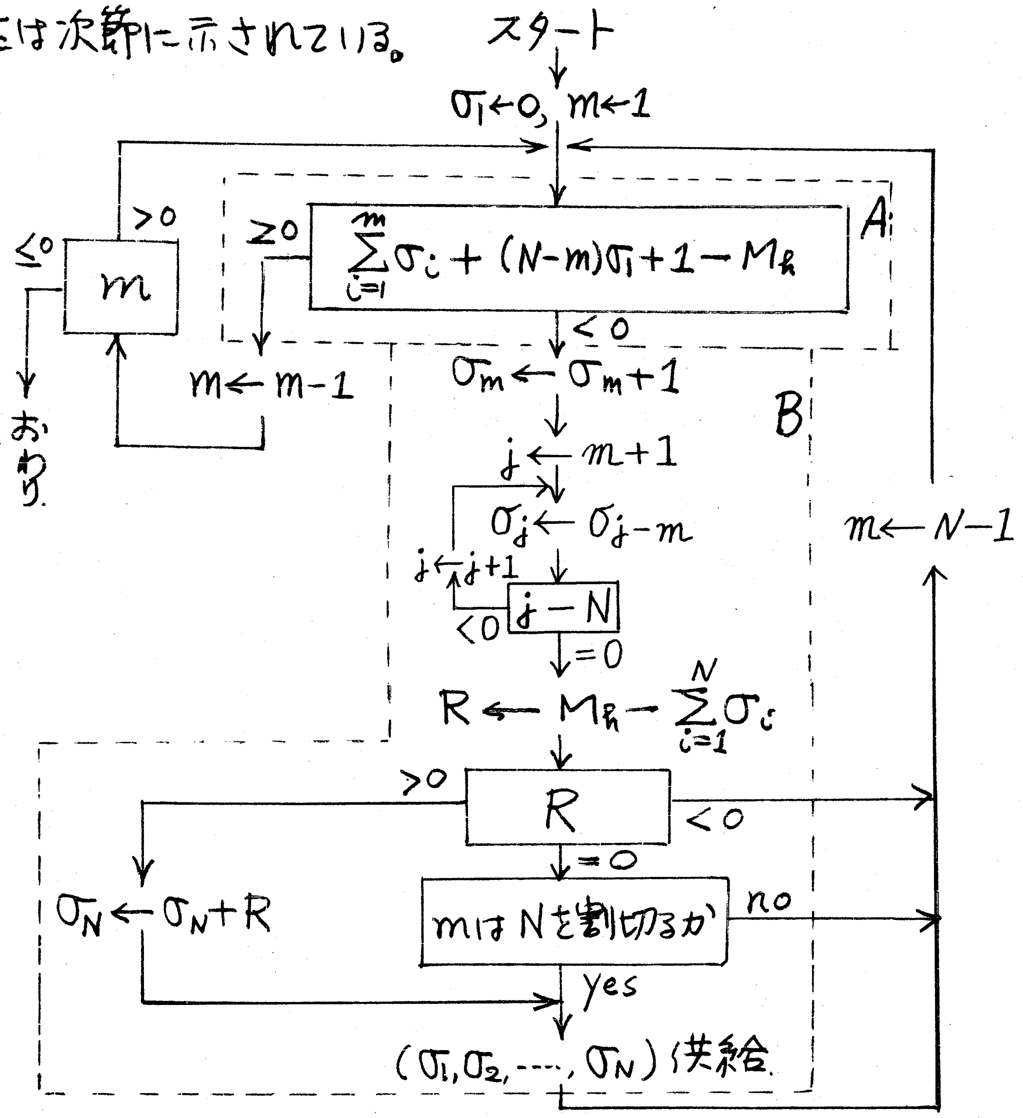
を考え，この系列で，サイクリックシフトで一致するものは

同等とし（図2参照），適当な方法で，それらの代表を1つずつとり，これをもとに，$s_1=0$，$s_2=\sigma_1$，$s_3=\sigma_1+\sigma_2$，…，$s_N=\sigma_1+\sigma_2+\cdots+\sigma_{N-1}$ の様にして $\{s_n\}$ を得ればよい。尚，上記代表を得るには次の流れ図に依ればよい．（図3）この図の正当性は次節に示されている。



円周のまわりは M_k 等分されている。

図2. σ_n と s_n



図中，$x \leftarrow y$ は，x に y という値を与えることを示す．

図3．$(\sigma_1,\sigma_2,\cdots,\sigma_N)$ の代表を供給する流れ図

§5. Cyclic Equivalence Classes

まず、"Cyclic Equivalence Class"と、その大きさの定義をする。

定義、

(1). $\sigma = (\sigma_1, \sigma_2, \cdots, \sigma_N)$を、$\sigma_i \geq 1$かつ$\sum_{i=1}^{N} \sigma_i = L$なる$\sigma_i$について定義し、$\sigma$の$j$個左cyclic shiftを

$$\sigma^j = (\sigma_1\ \sigma_2 \cdots\ \sigma_N)^j = (\sigma_j\ \sigma_{j+1} \cdots\cdots\ \sigma_{j-1})$$

と記す。

(2) σおよびそのCyclic shiftの全ての集合を、$C(\sigma)$と記し、これをσのCyclic Equivalence Class (CEC)と呼ぶ。単にC_1, C_2等とも記す。

(3) $P(\sigma) = \sum_{i=1}^{N} \sigma_i L^{N-i} = P(\sigma_1, \sigma_2, \cdots, \sigma_N)$を定義し、

$$\|C(\sigma)\| = \min_{\sigma' \in C(\sigma)} P(\sigma')$$ を$C(\sigma)$の大きさと言い、これによって$C(\sigma)$の大小を言う。

(4) $\|C(\sigma)\| = P(\sigma')$である$\sigma'$を、

$\sigma^c = (\sigma_1^c, \sigma_2^c, \cdots, \sigma_N^c)$と記し、Cの最小代表者とよぶ。

(5) $CL(\sigma_1^c, \sigma_2^c, \cdots, \sigma_m^c)$

$= \{C\ ;\ (\sigma_1^c, \sigma_2^c, \cdots, \sigma_m^c)$を最小代表者のはじめの部分とするもの、およびそれ以下の大きさを持つ全てのC$\}$

さて、これらの定義に基き、次の諸定理が成立つが、証明

は省く。

定理 1.) 各Cの最小代表者はただ1つきまり，かつ

$$C_1 = C_2 \iff \|C_1\| = \|C_2\|$$

系) 全ての $C \in \mathcal{C}$ を，その大きさの小さい順に並べることができ，どの2つも同じ大きさをもたない。

※この定理により，前節の $(\sigma_1, \sigma_2, \cdots, \sigma_N)$ の代表としては，上記にて $L = M_k$ とおき，Cの小さい順に求められた最小代表者を充当すればよい。

定理 2) Cの最小代表者を $\underline{\sigma}^c = (\sigma_1^c, \sigma_2^c, \cdots, \sigma_N^c)$ とすると，

(イ) $\sigma_i^c \geq \sigma_1$, $1 \leq i \leq N$

(ロ) もし，$\sigma_{i_1}^c = \sigma_1^c$ $2 \leq {}^{\exists}i_1 \leq N$ なら，$\sigma_{i_1+1}^c \geq \sigma_2^c$。もし更に等号が成立するなら $\sigma_{i_1+2}^c \geq \sigma_3^c$，以下同様。

定理 3) $CL(\sigma_1^c, \sigma_2^c, \cdots, \sigma_m^c)$ に含まれる全てのCより大きいCの最小代表者の最後の成分 $\sigma_N'^c$ は σ_1^c より大。

定理 4) $CL(\sigma_1^c, \sigma_2^c, \cdots, \sigma_m^c)$ に含まれる全てのCより大きいCとしては，次のものを最小代表者とするものより小さいものは存在しない。

$$\underline{\sigma}'^c = (\sigma_1^c, \sigma_2^c, \cdots, \sigma_{m-1}^c, \sigma_m^c+1, \sigma_1^c, \sigma_2^c, \cdots, \sigma_{m-1}^c, \sigma_m^c+1, \cdots\cdots, \sigma_1^c, \sigma_2^c, \cdots, \sigma_k^c, \sigma_N'^c)$$

但し，$k \leq m-1$ で，$\sigma_N'^c$ は，成分の和が L になる様に決められる。そして，事実これが，$CL(\sigma_1^c, \sigma_2^c, \cdots, \sigma_m^c)$

より大きい最小のCの最小代表者である為には，

$k \leq m-1$ ，$\sigma_N'^{c} > \sigma_{k+1}^{c}$ 又は，

$k = m-1$ 　$\sigma_N'^{c} = \sigma_m'^{c}$

のいずれかが成立することが必要十分である。

定理2と3が図3のAの部分を，また定理4がBの部分を説明する。

§6．最適化されたCGS．

§3～§5の方法で最適化されたCGSのパラメタの例を右表に示す。一般に，$\rho_{max} = \rho_{0\ell}$ である ℓ の値は2N個あるのが特徴である。

$M=47,\ N=4,\ R=0.694$		
$\rho_{max} = 0.345498$		
k_n	X_n	
1	0.287949	$\rho_{0\ell} = \rho_{max}$ である ℓ の値は
16	0.243621	4, 6, 12, 15
12	0.233615	32, 35, 41, 43
9	0.234814	

最適化されたCGSの内，任意の奇数のMに対し，$N = M_{\frac{1}{2}}$ としたものは，$X_n = 1/N$，$1 \leq n \leq N$，$\{k_n\} = \{1, 2, 3, \cdots, M_{\frac{1}{2}}\}$ とおいたものが最適であり，このとき，

$$\rho_{0\ell} = -1/2N = -1/(M-1) \quad (1 \leq \ell \leq M-1)$$ なので，

Regular Simplex 信号である。

尚，他の信号集合と比べる為，D. Slepian の方法[4]による評価を図4に示す。これは，最尤法による受信誤判定率 $P_e=$

10^{-5}とし，横軸に与えられた情報伝送速度を達成するに要する信号対雑音比(A)の，無限長符号の場合のそれ(Aideal)に対する相対値を縦軸にとったものである．図中，実曲線は，最適等エネルギ信号に関する下限[4]であり，点線で結んだ点はCGS，2点鎖線で結ばれている点はRegular Simplex信号，PMM nは，長さnのPermutation Modulation，[5] BO nは長さnの陪直交信号を示す。

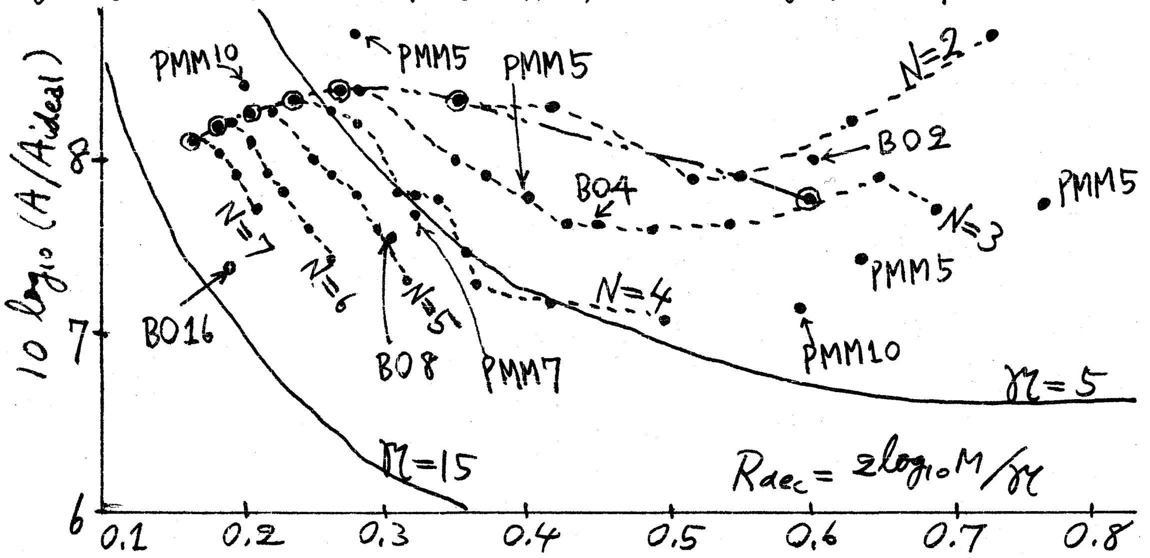


図4．D. Slepianの方法による評価，$P_e=10^{-5}$.

§7．むすび．

次元が少し大きくなると上記の方法は実行不能になる．[3]によればMは素数の必要はないので，素数の場合の組合せで良い信号を得る可能性を検討中である．

文献：〔1〕伊藤：電子通信学会論文誌（B），**51-B**，3，P111（昭43-03）．〔2〕伊藤，水町，川本：電子通信学会全国大会，**20**（昭43-10）．〔3〕伊藤，水町，川本：電気四学会連合大会，**2954**（昭44-03）．〔4〕D. Slepian：BSTJ，**42**，p681（May 1963）．〔5〕D. Slepian：Proc. IEEE，**53**，3，p228（March 1965）．