京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

京都大学
KYOTO UNIVERSITY

Title	基本群と符号理論(離散数理モデルにおける最適組合せ構造)
Author(s)	今井, 潤
Citation	数理解析研究所講究録 (1993), 820: 157-162
Issue Date	1993-02
URL	http://hdl.handle.net/2433/83164
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

Kyoto University

数理解析研究所講究録
第820巻 1993年 157-162

基本群と符号理論

今井 潤
Jun IMAI
NTT コミュニケーション科学研究所
NTT Communication Science Laboratories

1 序論

1989年、J. A. Wood は「SO(n) の被覆空間 Spin(n) の diagonal extra-special 2-group の abelian 2-subgroups は任意の self-orthogonal linear binary code of block n と対応関係があり、特に even self-orthogonal code に関しては、Spin(n) の equivariant cohomology ring の prime ideal と 1対1の対応がある。また equivalence classes of maximal doubly-even self-dual codes は $H^*(BSpin(n), Z_2)$ の minimal prime ideal と1対1の対応がある。」という結果を発表した。方法は前者に関しては 2次形式の Clifford theory を用いて直接対応をつけ、後者については Lie group の分類空間の equivalent cohomology に関する Borel, Serre, Quillen 等による結果、特に cohomology の elementary abelian p-group に関する結果を全面的に引用し、その系として導いている。またその応用として Morse theory を用いて cohomology ring の prime ideal を調べることによって self-orthogonal code の情報を得ることができることを述べている。本研究は上記の結果をすべての符号に対して一般化することを最終目的としている。その一般化された符号を特徴づけるために、まず考えるのが次節で述べる第一基本原理である。

2 符号理論の第一基本原理

まず最初に議論するのは、与えられた条件を満足する符号を構成するのに必要な指導的原理と、その結果得られた符号あるいは符号族の持つ情報の所在をしめす基本原理である。この原理は、すべての符号（あるいは符号族）が本来所有している性質を明確に認識するために必要となる。またこの性質を理解するために一般化が必要となる。

第一基本原理 $\mathcal{G}$;the category of codes, $\mathcal{X}$;the subcategory of covering spaces with covering transformation group (or the subcategory of principal bundle) とする。この時つぎの 1., 2., 3., 4. の性質を満たす対応 $\mathrm{F} : \mathcal{G} \longrightarrow \mathcal{X}$,$\mathrm{G} : \mathcal{X} \longrightarrow \mathcal{G}$ が存在する。

1. $C \in Ob(\mathcal{G})$ に対して、

$$\mathrm{F}(C) : \tilde{X} \longrightarrow X; (\text{the covering space with some transformation group } C')$$

such that: $\tilde{X}$;connected
$\mathrm{F}(C)_*(\pi_1(\tilde{X}))$; normal in $\pi_1(X)$
$\pi_1(X)/\pi_1(\tilde{X}) \cong C'$
C' は $\tilde{X}$ 上に自由に作用する。(acts freely on $\tilde{X}$)
C' は C の $Cokernel$
$\pi_0(\tilde{X}) \approx Cokernel(C)$

2. $Y \in Ob(\mathcal{X})$ に対して、その base space を X とするとき $\mathrm{G}(Y)$;code such that

$$[X, BCokernel(\mathrm{G}(Y))] \approx Hom(\pi_1(X), Cokernel(\mathrm{G}(Y))) \ (bijective)$$

またこの時、Y に対応する classifying map を φ とすると、

$$\pi_0(\tilde{X}) \approx Cokernel(\mathrm{G}(Y))/im(\varphi)$$

3. bijectivity;

$$\mathrm{G}(\mathrm{F}(C)) = C,\ \mathrm{F}(\mathrm{G}(Y)) = Y \quad \text{for any } C \in Ob(\mathcal{G}) \text{ and } Y \in Ob(\mathcal{X})$$

4. 任意の $C \in Ob(\mathcal{G})$ に対し、ある $\mathcal{F}$ が存在し、Z を $\mathrm{F}(C)$ の universal covering space とするとき、コホモロジー環 $H^*(BZ, \mathcal{F})$ が符号 $C \in Ob(\mathcal{G})$ を部分符号に持つある符号の、あるいは C を部分集合に持つある符号族に関する全ての情報を含む。但し、$\mathcal{F}$ は適当な群あるいは、局所係数、または層を意味するものとする。

但し、$B*$ は、$*$ の classifying space を 表し、群 C の free action とは、

$$gx \neq x \text{ for all } x \in X \text{ and } g \neq 1 \text{ in } C$$

を意味する。

この原理は従来の符号の概念、従来の符号のカテゴリーでは定義もできないし、かつ理解不能である。本論文の目標は、この原理が成立するように、符号の概念を、従来の符号の概念をふまえて一般化し、その結果として符号の構成や、復号、そして符号の持っている性能の分析を明解に行なえるようにすることにある。符号の一般化・復号については既に著者により与えられているので、本稿では、上記原理を満たすような covering space のモデルとして如何なるものを取ることができるかについて考察する。

モデルの取り方として、考えられる方法は2通りある。抽象的な同変複体を用いる構成方法と、低次元複体による構成方法である。後者を議論する必然性としては、次の様な事が考えられる。

- 第一基本原理の主張から、高次元の部分はおおきな影響を持たないはずである。
- 符号が具体的な1次元複体と関係が付けられれば、符号を評価する新しい明解な尺度となりうる。

なおこの研究において、符号理論の第二基本原理と呼ばれる主張は、復号の原理に関するものである。(imai 1992)

3 第一基本原理の正当性

先ず、線形符号とは群である。しかもより大きな群に部分群として埋め込まれており、かつ、大きい群の位相に関して、埋め込まれた群の元どうしはある距離以上離れているという状況にある。つまり、距離を考慮しなければ群の拡大を考えていることになる。具体的には適当な体上の線形空間における超平面群の共通部分（連立方程式の解集合）であるから、群の拡大がカテゴリーとして大き過ぎるならば一般の加群の短完全系列に制限してもよい。加群で重要な概念であるのが自由性 (free) であるが、環上の加群を議論するのならば射影的 (projective) を自由性の代わりに考慮するのが自然であり、群の拡大なら、分裂性を考慮するべきである。このような代数的な範疇で議論をする場合、我々に与えられた道具は群のコホモロジーであり、Grothendieck group (algebraic K-theory) である。この部分の議論については既に著者により不完全ではあるが議論されている。しかし、代数的な範疇を越える時には前節に述べたような原理が成立し得るはずである。なぜなら、第一基本原理に述べたことは代数の世界で成立することを、vector bundle (topological K-theory) という幾何学的な世界での表現に置き換えることによって得られるべき事実が中心となっているからである。但し、幾何学的な世界も非常に広いので、完全に一般化してしまうと有用な性質が見えなくなる虞があるので、principal bundle (covering space) に制限している。この世界では、射影性は局所自明性に置き換わり、幾何学的な resolution により定義される幾何学的なコホモロジー群が存在し、幾何学的世界において固有な現象である群の作用を考慮するとき群のコホモロジーとの関係が生じ、その顕著な場合が K(G,1) (Eilenberg-Maclane space) である。このように符号（群）に幾何学的世界における対応する対象を考えた場合に特徴的な現象は群の作用の存在である。そして vector bundle には universal bundle (universal covering) を考えることで同類の対象をひとまとめに考察できる。(classical algebraic K-theory では universal central extension に対応する。) これは作用する群を G とすれば、

$$G \longrightarrow EG \longrightarrow BG$$

と書ける。但し EG は群 G の無限個の join から作られる空間で、BG はそれを G の作用で割ったものであり、分類空間と呼ばれる。（この例は G は位相群で、bundle は principal G-bundle であるものとする。）分類空間の特徴は、任意の底空間 X の G-bundle の同値類を homotopy class $[X, BG]$ で特徴付けることができることであり

$$H^n(G, R) \cong H^n(BG, R) \ for\ \forall R$$

となることである。もしCW-complex でBGをとるならば、これは先ほどの $K(G,1)$ である。ここで注意すべき点は、この空間のホモトピー群が基本群を除いて自明である事である。つまり1次元的な部分のみが本質的で、高次元の部分はある意味で自明な幾何学的対象によって bundle は分類できるという事実が重要である。このことは代数的、幾何学的という2極的構造に付け加えて、組合せ論的構造という第3の構造が付随していることを示唆している。1番目、2番目の構造が、ある対象の異なる側面を記述しているのに対し、第3の構造はそれらを繋げる具体的操作に関する情報を与える。以上をまとめると次の様になる。

1. 群の拡大あるいは加群の短完全系列
2. principal G-bundle あるいは covering space
3. graphs with group action

が基本的な三角形を形成している。さらにこの時、

- (1)、(3)を関係づける対応:graph of groups, graph automorphism group
- (1)、(2)を関係づける対応:fundamental group, genus, algebraic and topological K-theory (from (1) to (2) :B* ,from (2) to (1): covering transformation group)
- (2)、(3)を関係づける対応:topological structures of graph and $Z_p$structure of cohomology

のようになっていると考えられる。

そして、Wood の結果は self-orthogonal code に(1)を限定すると、

$$K(\mathrm{Z}_2,1) \longrightarrow BSpin(n) \longrightarrow BSO(n)$$

という bundle あるいは universal covering space に対応していることを具体的に示したものといえる。また同時にある種の有用な符号のクラスは spin structure と関係があり、self-orthogonality は 4次元多様体論の ゲージ理論的研究と関係を持っていることも意味している。

4 実用的な符号に対する例

self-orthogonal codes over F_2 の場合
まずこの符号をカテゴリー(2)において特徴付ける。このために次の事実に注意する。

Definition 4.1 (ordinary code) 従来の符号理論は(線形符号に関する限り)次のような *short exact sequence* で表すことができる。

$$0 \longrightarrow \boldsymbol{K}^l \xrightarrow{\varphi} \boldsymbol{K}^{n+l} \xrightarrow{\psi} \boldsymbol{K}^n \longrightarrow 0 \ (exact)$$

ここで、この系列に現れる単射を φ, 全射を ψ とし、適当な基底に対するその行列表示をそれぞれ G, H とするとき、Hを *parity check matrix* と呼び、また、Gを符号の *generator matrix* と呼ぶ。

Proposition 4.1 (Classifying Theorem for ordinary codes) *G(n+l, l)* を冗長度 n を持つ情報記号長 l の線形符号全体の集合とする。このとき、以下が成立する。

$G(n+l,l) \subset [X, x_0; BG, *]$ *(the group of homotopy class for some space X to classifying space of some Group G)*

Proof: 上に定義された符号を別の立場で、観察してみる。

$$0 \longrightarrow \boldsymbol{K}^l \xrightarrow{\varphi} \boldsymbol{K}^{n+l} \xrightarrow{\psi} \boldsymbol{K}^n \longrightarrow 0 \ (exact)$$

今、$\boldsymbol{K}^{n+l}$ において $\boldsymbol{K}^l$ の元 v は、$\psi^{-1}(p)$ に推移的に作用している(例えば、v による平行移動)。また $\boldsymbol{K}^{n+l}$ は ψ の section と $\boldsymbol{K}^l$ の直積で表現されていると見ることができる。すなわち

$$\tilde{X} := \boldsymbol{K}^{n+l},\ X := \boldsymbol{K}^n,\ G := \boldsymbol{K}^l$$

と見ると、$\tilde{X} \longrightarrow X$ は pricipal G-bundle あるいは、covering space with deck transformation group G, と解釈することができる。(位相を考慮しない場合には、principal homogeneos G-set になる。) この場合には、G の適当な線形表現を考え、その像をあらためて G と考える。従って分類定理により、符号は $[X, x_0; BG, *]$ の元とみなすことができる。
上の主張より、通常の線形符号を被覆空間あるいは pricipal G-bundle と対応させることが可能となる。もっと詳しく述べると、$GL(n)$ の部分群を構造群とする bundle である。次に、self-orthogonal code を次のように特徴付ける。

Definition 4.2

$$1 \longrightarrow N \longrightarrow G \longrightarrow E \longrightarrow 1(exact)$$

但し、N :*cyclic of order 2*, E :*elementary abelian 2-group of order* 2^n *(extraspecial 2-group)* また、*quadratic form* $q : E \longrightarrow N$ を $x \in E$ の 逆像 $\tilde{x} \in G$ の 2 乗で与え、*symmetric bilinear form* $b : E \times E \longrightarrow N$ を以下の様に定義する。

$$b(x, y) := (\tilde{x}\tilde{y})^2 = \tilde{x}^2\tilde{y}(\tilde{y}^{-1}\tilde{x}^{-1}\tilde{y}\tilde{x})\tilde{y} = \tilde{x}^2\tilde{y}^2\,[\tilde{x}, \tilde{y}]$$

(Definition 終り)

この時、次がわかる。

$$H^*(E, \mathrm{F}_2) = \mathrm{F}/2(x_1, ..., x_n), deg(x_i) = 1$$

そして上の central extension を決める特性類は

$$q(v) \in H^2(E, \mathrm{F}_2), v \in V := k \otimes_{F_2} E$$

但し k は標数 2 の代数的閉体である。
また、$e_1, ..., e_n$ を E の F_2 上の基底とし、$v = \sum_{i=1}^n x_i e_i$ とする時、

$$q(v) = q\left(\sum_{i=1}^n x_i e_i\right) = \sum_{i=1}^n q(e_i)x_i^2 + \sum_{1 \le i < j \le n} b(e_i, e_j)x_i x_j .$$

今、$k[V]$ 上の Frobenius map を F と書く時、これは x_i を x_i^2 へ写す k-linear ring homomorphism になる。この時、次が成立する。

Theorem 4.1 (Quillen) G を上で与えられた群とするとき

$$H^*(G, F_2) = F_2[x_1, ..., x_n]/(q(v), b(v, F(v)), ..., b(v, F^{h-1}(v))) \otimes F_2[\zeta]$$

但し、$deg(x_i) = 1$,x_i は $H^*(E, F_2)$ からの *inflation map* の像。整数 h は *maximal* F*-stable isotropic subspace* の V における *codimension.* (言い替えると、2^h は G における *maximal elementary abelian subgroup* の *index.*)
ζ は $H^*(N, F_2)$ への *ristriction map* による像が自明でない任意の *degree* 2^h の元である。また

$$b(v, F^j(v)) \in (q(v), b(v, F(v)), ..., b(v, F^{h-1}(v))), (j \ge h)$$

(Theorem 終り)

Remark: Wood は 最初から、以下のような位相群の完全系列を self-orthogonal code を特徴付けるために用いた。

$$0 \longrightarrow \mathrm{Z}_2 \longrightarrow Spin(n) \longrightarrow SO(n) \longrightarrow 0(exact)$$

これは Clifford theory を用いて議論しているためであり、かつ Quillen の Lie group の分類空間の Z_p-cohomology に関する計算結果を利用するためであった。しかし、後で述べる様にカテゴリー (2) へ写すと上で与えたものの像と同値な bundle になる。本稿では各カテゴリー間の対応を明確にするために上記のような特徴付けをした。また Lie group で特徴付けると、各カテゴリーにおけるオブジェクトに明確な違いが出ないことが多いという理由 (位相群はそれ自体が幾何学的対象)、また cohomology も幾何学的なものを用いるか代数的なものを用いるかを明確にしたいという理由もある。。逆に、このような Lie group の完全系列は符号理論的に非常に重要なオブジェクトであるとも言える。(Remark 終り)

次に、カテゴリー（1）から（2）への対応を考える。出発点となる central extension は universal なものだから、（2）においても universal なものが対応することが望ましい。この部分の対応は K-theoretical に 各群の分類空間をとるという操作を採用する。すると以下の fibration が得られる。

$$BZ_2 = K(Z_2, 1) \longrightarrow BG \longrightarrow BE(universal)$$

以下第一基本原理の 4番目の主張が満たされることを見ることにする。先ず Quillen, Borel による compact Lie group の cohomology ring に関する性質をまとめておく。

Theorem 4.2 (Borel) *G:a compact connected Lie group*

1. $H^*(G;Z)$ は *p-torsion* を持たないならば、$H^*(G;Z_p)$ は *exterior algebra of a graded vector space with generators of odd degree* となる。
2. $H^*(G;Z)$ が *torsion free* ならば $H^*(G;Z)$ は *exterior algebra of a free abelian group* であり、その基底はすべて、*odd degree* の元からなる。この時生成元の数は G の *rank* に等しい。
3. $H^*(G;Z_p)(resp.H^*(G;Z))$ が *exterior algebra of a vector space (resp. free abelian group)* かつ、その生成元の *degree* は全て奇数 $r_1,...,r_l$ であったとすると、$H^*(BG;Z_p)(resp.H^*(BG;Z))$ は $Z_p(resp.\ Z)$ 上の *polynomial algebra* であり、その生成元の *degree* は $r_1+1,...,r_l+1(even\ degrees)$ となる。

(Theorem 終り)

Theorem 4.3 (Quillen) *G:a compact Lie group*

$$H_G := \oplus_{i\geq 0} H^*(BG;Z_p), (p = odd)\ H_G := \oplus_{i\geq 0} H^*(BG;Z_2), (p=2)$$

とおく。この時、以下が成立する。

1. $dim H^*(BG;Z_p)$ =*the maximum rank of an elementary abelian p-subgroup of* G $(Z_p - tori)$
2. $A{:}Z_p - torus\ in\ G$
$$\phi_A : H_G \to H_A \to H_A/\sqrt{0} = S(H^1(BA;Z_p))$$
の *kernel* を p_A とする時、これは *prime ideal* である。
3. $A, A'{:}Z_p - tori\ in\ G.$
(1)$p_A \subset p_{A'}$ *if and only if* A *is conjugate to a subgroup of* A'. *(2)*$p_A = p_{A'}$ *if and only if* A *is conjugate to* A'. *(3)map (from maximal* $Z_p - torus\ A$ *in* G *into the prime ideal* p_A*)* は *conjugacy classes of maximal* $Z_p - tori\ in\ G$ と *minimal prime ideals in* H_G の間の1対1対応を誘導する。
4. H_G の *prime ideal* が $p_A(A : Z_p - torus)$ の形で表現されるための条件は H_G が *homogeneous* かつ *Steenrod operation* に対して安定であることである。
5. J: 以下の *regular sequence* から生成された $H^*(BSO(n);Z_2)$ の *ideal.*
$$w_2, Sq^1 w_2, \ldots, Sq^{2^{h-1}} Sq^{2^{h-2}} \cdots Sq^1 w_2,$$
ここで w_2 は *2nd universal Stiefel-Whitney class,* また Sq^i は *Steenrod operator.* Δ_θ を *spin representation of Spin(n)* とする。この時、以下は同型である。
$$H^*(BSO(n);Z_2) \otimes (Z_2)[w_{2^h}(\Delta_\theta)] \to H^*(BSpin(n);Z_2).$$

(Theorem 終り)

以上の準備から以下の結果が導かれる。

Theorem 4.4 第一基本原理の4番目の主張は *self-orthogonal code* に対して満たされる。

参考文献

Proof: Definition 4.2 で与えた central extension において、$H^*(BG;\mathrm{Z}_2)$ が self-orthogonal code に関する情報を持っていることを示す。G は discrete group で、$BG = K(G,1)$ であるから、

$$H^n(BG;\mathrm{Z}_2) \cong H^n(K(G,1);\mathrm{Z}_2) \cong H^n(G;\mathrm{Z}_2)$$

また Theorem 4.1 において、$q(v), b(v,F(v)), ..., b(v,F^{h-1}(v))$. が regular sequence であることと、

$$b(v,F^r(v)) = \sum_{1\leq i<j\leq n} b(e_i,e_j)(x_i x_j^{2^r} + x_j x_i^{2^r}) \doteq Sq^{2^{r-1}} Sq^{2^{r-2}} ... Sq^1 q(v)$$

となることが容易に確認できる。従って、

$$H^*(BSO(n);\mathrm{Z}_2) \cong \mathrm{Z}_2[w_2, w_3, ..., w_n]$$

に注意すると、Theorem 4.1 と Theorem 4.3 から

$$H^*(BG;\mathrm{Z}_2) \cong H^*(BSpin(n);\mathrm{Z}_2)$$

が示され、ここで Wood の結果を用いれば、$H^*(BG;\mathrm{Z}_2)$ が所記の性質を持つことがわかる。(proof 終り)
Remark: bundle

$$B\mathrm{Z}_2 = K(\mathrm{Z}_2,1) \longrightarrow BG \longrightarrow BE$$

は universal 故、前 Remark において予告した事が同時に示された。また、底空間 $BSO(n) = Gr(n,\infty)$ すなわち、n-planes in R^∞ から成る Grassmann variety となる。この事は Proposition 4.1 の事実に呼応する。なぜなら、線形符号の構造群 G は GL(n) の部分群であり、かつ $BG \cong BGL(n) \cong BSO(n) \cong Gr(n,\infty)$ だから、線形符号に関しては、カテゴリー (2) において、Grassmannian を 底空間とする canonical bundle を分類写像で引き戻したものが対応しているべきであるからである。(Remark 終り)

5 (1)と(3)の関係

(1)、(3)を繋げる具体的理論としては、graph of groups を用いて定義した G-tree (tree with group action) が有用である。具体的には拡大したい群 G の作用する connected G-graph X を考え、これから graph of groups を構成し、群の拡大をこの graph of groups の fundamental group を用いて構成する。この時やはり graph covering が生じ、(1)と(2)の間の関係に類似した現象が現れる。また低次元 complex から生じる cohomology を考慮すると(1)、(2)の対応関係を凝縮した様なモデルとなる。また covering の分岐に着目した復号法も考えられる。これらの議論の詳細については本稿の拡張版において説明する予定である。

参考文献

[1] Wood, J. A. *Spinor groups and algebraic coding theory*, Journal of Combinatorial Theory, Series A 1989.

[2] Quillen, D. *A cohomological criterion for p-nilpotence*,J. Pure Appl. Algebra 1, 1971. 361-372

[3] Quillen, D. *The mod 2 cohomology rings of extra-special 2-groups and the spinor groups*, Math. Ann. 194, 1971, 197-212

[4] Borel, A. *Sur la cohomologie des espaces fibrés principaux et des espaces homogènes de Lie compacts*, Ann. Math. (2) 57 ,1953, 115-207

[5] Borel, A. *Sous-groupes commutatifs et torsion des groupes de Lie compacts connexes*, Tôhoku Math. J. 13, 1961, 216-240

[6] Imai, J. *A generalization of coding theory and covering space*, preprint

[7] Imai, J. *Galois representations and error-correcting codes*, preprint

[8] Freed, D. S., Uhlenbeck, K. K. *Instantons and Four-manifolds*, Springer-Verlag 1984.

[9] Serre, J. -P. *Trees*,Springer-Verlag 1980.