数理解析研究所講究録 1228 巻 2001 年 51-60

小関多項式と符号の被覆半径の計算

田辺顕一朗 (Kenichiro Tanabe)
筑波大学数学系
Institute of Mathematics, University of Tsukuba
e-mail:tanabe@math.tsukuba.ac.jp

1 イントロダクション

この講演では原田昌晃、小関道夫との共同研究 [2] で行った、符号の被覆半径およびコセット重み枚挙多項式の小関多項式を用いた計算について話します。方針は小関 [5] と同じですが、ある有限群の不変式環に関する結果を用いてより大きな長さの符号に対してそれらの値が計算出来るようになったことが特徴です。コセット重み枚挙多項式に関しては今まで知られていた方法 (補題 1 参照) よりは符号によっては、より少ない労力で計算が出来るようになります。

1997 年、小関 [4] によって符号の小関多項式が導入されました。論文 [4] の中では小関多項式は Jacobi 多項式と呼ばれていますが、全く別の多項式に対して既に同じ名前が付けられていることもありここでは小関多項式と呼ぶことにします。

最初に符号に関して紹介しておきます。三元体 $\mathbb{F}_3$ 上の n 次元ベクトル空間 $\mathbb{F}_3^n$ の部分空間 C を三元体上の長さ n の線形符号と呼びます。他の有限体に対しても符号は同様に定義できますが、ここでは三元体上の線形符号しか扱いません。以下簡単に三元体上の線形符号 C のことを符号と呼びます。

$a=(a_k), b=(b_k) \in \mathbb{F}_3^n$ と $i,j \in \{0,1,2\}$ に対して、記号 $\mathrm{wt}(a) := |\{k \mid a_k \neq 0\}|$ と $\mathrm{wt}_{ij}(a,b) := |\{k \mid a_k = i \text{ and } b_k = j\}|$ を準備します。また内積 $(a,b) := \sum_{k=1}^n a_k b_k$ を定義します。符号 C に対してその直交空間 $C^\perp := \{a \in \mathbb{F}_3^n \mid (a,c) = 0, \text{ for all } c \in C\}$ を定義します。$C = C^\perp$ を満たす符号 C は self-dual であると呼ばれます。商ベクトル空間 $\mathbb{F}_3^n/C$ の元 U を C のコセットと呼びます。また $W_U(x) = \sum_{u \in U} x^{\mathrm{wt}(u)}$ をコセット重み枚挙多項式と呼びます。$a \in U$ が $\mathrm{wt}(a) \leq \mathrm{wt}(b)$ $(^\forall b \in U)$ を満たす時、a は U のコセットリーダーであると呼ばれます。コセットリーダーの重みをそのコセットの重みと呼ぶことにします。

符号 C に対して、

$$\mathbb{F}_3^n = \cup_{c\in C}\{a \in \mathbb{F}_3^n \mid \mathrm{wt}(a-c) \le r\}.$$

を満たす非負の整数 r の最小値を符号の被覆半径と呼び、ここでは $\rho(C)$ で表すことにします。与えられた符号に対してその被覆半径を決定するのは符号理論における重要な問題の一つです。簡単に

$$\rho(C) = \max_{a\in\mathbb{F}_3^n}\min_{c\in C}\mathrm{wt}(a+c)$$

が示せます。これから全ての $a \in \mathbb{F}_3^n$ に対して $W_{a+C}(x)$ が分かれば、$\rho(C)$ が決定できまることに注意します。符号の被覆半径の計算には次の結果が有用です。

補題 1 (Delsarte[1])

(1) $\rho(C) \le |\{\mathrm{wt}(a) \mid 0 \ne a \in C^\perp\}| =: D(C)$ が成り立つ。$D(C)$ は Delsarte bound と呼ばれる。
(2) $W_{a+C}(y)$ の $D(C)-1$ 次までの係数が分かれば $W_{a+C}(y)$ は計算出来る。

(1) から各 $a \in \mathbb{F}_3^n$ に対して $\min_{\beta\in a+C}\mathrm{wt}(\beta) \le D(C)$ が分かります。したがって全ての $a \in \mathbb{F}_3^n$ ではなく、$\mathrm{wt}(a) \le D(C)$ となる全ての $a \in \mathbb{F}_3^n$ に対して $W_{a+C}(y)$ を計算すれば良いことが分かります。また $\mathrm{wt}(c) \ge \mathrm{wt}(a)+D(C)$ ならば $\mathrm{wt}(a+c) \ge \mathrm{wt}(c)-\mathrm{wt}(a) \ge D(C)$ に注意すると、(2) から $P_a(C) := \{c \in C \mid \mathrm{wt}(c) < \mathrm{wt}(a)+D(C)\}$ に対して $\sum_{\beta\in P_a(C)} x^{\mathrm{wt}(\beta)}$ を計算すれば $W_{a+C}(x)$ を決定出来ることが分かります。

小関多項式の紹介をします。$a \in \mathbb{F}_3^n$ と符号 C に対して x, y, u, v, w を変数とする多項式

$$\begin{aligned} & O(C, a; x, y, u, v, w) \\ := & \sum_{c\in C} x^{\mathrm{wt}_{00}(a,c)} y^{\mathrm{wt}_{01}(a,c)+\mathrm{wt}_{02}(a,c)} \\ & \times u^{\mathrm{wt}_{10}(a,c)+\mathrm{wt}_{20}(a,c)} v^{\mathrm{wt}_{11}(a,c)+\mathrm{wt}_{22}(a,c)} w^{\mathrm{wt}_{12}(a,c)+\mathrm{wt}_{21}(a,c)} \end{aligned}$$

を a に関する C の小関多項式と呼びます。

a	0			1			2		
c	0	1	2	0	1	2	0	1	2
$a+c$	0	1	2	1	2	0	2	0	1
	x	y	y	u	v	w	u	w	v

小関多項式において変数を以下のように置き換えると、

$$\begin{aligned} & O(C,a;1,x,x,x,1) \\ = & \sum_{c\in C} x^{\mathrm{wt}_{01}(a,c)+\mathrm{wt}_{02}(a,c)+\mathrm{wt}_{10}(a,c)+\mathrm{wt}_{20}(a,c)+\mathrm{wt}_{11}(a,c)+\mathrm{wt}_{22}(a,c)} \\ = & \sum_{c\in C} x^{\mathrm{wt}(a+c)} = W_{a+C}(x). \end{aligned}$$

となり、コセット重み枚挙多項式 $W_{a+C}(x)$ が計算できます。したがって小関多項式が分かれば、符号の被覆半径が決定できます。

以上小関多項式から符号の被覆半径及びコセット重み枚挙多項式が得られることを見てきたわけですが、一般に与えられた符号に対してその小関多項式を計算するのは困難な問題です。しかし以下に見るように符号が self-dual である場合には有限群の不変式論の方から小関多項式に関する情報を得ることが可能になります。まず次の結果が成り立つことに注意します。

補題 2 (小関 [5]) C が self-dual ならば小関多項式は次の行列の作用の下で不変である。

$$L_1 := \frac{1}{\sqrt{3}} \left[\begin{array}{cc|ccc} 1 & 1 & 0 & 0 & 0 \\ 2 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & \omega^2 & \omega \\ 0 & 0 & 1 & \omega & \omega^2 \end{array}\right], \text{ and}$$

$$L_2 := \mathrm{diag}(1,\omega,1,\omega,\omega),$$

ここで $\omega := e^{2\pi\sqrt{-1}/3}$. さらにもし $C \ni (1,\ldots,1)$ ならば $L_3 := \mathrm{diag}(\omega,1,\omega,1,1)$ でも不変となる。

上の補題から小関多項式は不変式環 $\mathbb{C}[x,y,u,v,w]^{\langle L_1,L_2\rangle}$、または $\mathbb{C}[x,y,u,v,w]^{\langle L_1,L_2,L_3\rangle}$ の元となるわけですが、これらの不変式環について次の結果が得られています。

補題 3 (田辺 [6]) $\mathbb{C}[x,y,u,v,w]^{\langle L_1,L_2\rangle}$ と $\mathbb{C}[x,y,u,v,w]^{\langle L_1,L_2,L_3\rangle}$ の生成元を具体的に与えることが出来る。

より正確には、例えば $\mathbb{C}[x,y,u,v,w]^{\langle L_1,L_2,L_3\rangle}$ の場合には次の $\{\eta_i\}$ 達を具体的に与えることが出来ます:

$$\begin{aligned} & \mathbb{C}[x,y,u,v,w]^{\langle L_1,L_2,L_3\rangle} \\ & = \oplus_{i=1}^{864} \eta_i \mathbb{C}[\theta_1,\theta_2,\theta_3,\theta_4,\theta_5]. \end{aligned}$$

$$\begin{aligned}
\theta_1 &:= (x^4+8xy^3)^3.\\
\theta_2 &:= (x^6-20x^3y^3-8y^6)^2.\\
\theta_3 &:= (4u^4+4u(v+w)^3)^3.\\
\theta_4 &:= (8u^6-20u^3(v+w)^3-(v+w)^6)^2.\\
\theta_5 &:= (v-w)^{12}.
\end{aligned}$$

2 符号の被覆半径の計算

$\mathbb{F}_3$ 上の extremal self-dual code は長さ 24 までは分類されています (特に長さ 24 の符号は二つ)。長さ 28 は 32 個以上あることが知られています。プレプリント [2] では補題 3 を用いて長さ 24 の二つ、また Huffman[3] が構成した長さ 28 の extremal self-dual code の小関多項式 (結果としてコセット重み枚挙多項式と被覆半径も) を計算しました。実はそれらの符号の被覆半径は既によく知られていて、そちらに関しては新しい結果ではありません。コセット重み枚挙多項式に関しては新しい結果です。長さ 32 以上は計算量が多すぎて今のところ出来ていません。

Extremal self-dual codes/$\mathbb{F}_3$

長さ	コセット重み枚挙多項式
≤ 12	Known
16, 20	小関道夫 [5]
24	原田昌晃, 小関道夫, 田辺 [2]
Huffman, 28	原田昌晃, 小関道夫, 田辺 [2]
≥ 32	?

ここでは長さ 28 の場合を例に取り、計算方法を紹介します。$a \in \mathbb{F}_3^{28}$ s.t. $\mathrm{wt}(a) = i$ に対して小関多項式 $O(a, C; x, y, u, v, w)$ を計算していきます。補題 1 (1) から $\mathrm{wt}(a) \leq D(C) = 7$ まで決めればよいことに注意します。まず補題 3 から可能な小関多項式を求めておきます。

(1) 次数 28 の斉次不変式

$$\begin{aligned}
&f \in R := \mathbb{C}[x, y, u, v, w]_{28}^{\langle L_1, L_2, L_3\rangle},\\
&(f \text{ の変数 } u, v, w \text{ に関する次数}) = i.
\end{aligned}$$

を補題 3 で得られている R の生成元を使ってパラメータ付きで表す。

それを

$$f = \sum_{n_x,n_y,n_u,n_v,n_w} \gamma_{n_x,n_y,n_u,n_v,n_w} x^{n_x} y^{n_y} u^{n_u} v^{n_v} w^{n_w}.$$

$$\gamma_{n_x,n_y,n_u,n_v,n_w} \in \mathbb{C}.$$

と展開しておく。

(2) $d := \min\{\mathrm{wt}(c) \mid 0 \neq c \in C\}$ とおくと C は extremal であるから $d = 3\lfloor n/12 \rfloor + 3$ となる。この事に注意して、条件

(i) $f(1,1,1,1,1) = |C|$.

(ii) $n_y + n_v + n_w < 3\lfloor n/12 \rfloor + 3 \Longrightarrow \gamma_{n_x,n_y,n_u,n_v,n_w} = 0$.

から係数のパレメータの数を減らす。

例えば $\mathrm{wt}(a) = 6$ の場合は次のようになります。表に載っていないその他の係数もパラメータ $s_2, \ldots, s_{10}$ を用いて表せます。

$\mathrm{wt}(a) = 6$ の可能な小関多項式

x	y	u	v	w	$\mathrm{wt}(a+c)$	$\mathrm{wt}(c)$	係数
22	0	6	0	0	6	0	1
19	3	0	0	6	3	9	s_{10}
19	3	0	1	5	4	9	s_9
19	3	0	2	4	5	9	s_6
19	3	0	3	3	6	9	s_3
19	3	0	4	2	7	9	s_6
19	3	0	5	1	8	9	s_9
19	3	0	6	0	9	9	s_{10}
18	4	1	0	5	5	9	s_7
18	4	1	1	4	6	9	s_5
18	4	1	2	3	7	9	s_2
18	4	1	3	2	8	9	s_2
18	4	1	4	1	9	9	s_5
18	4	1	5	0	10	9	s_7
17	5	2	0	4	7	9	s_8
17	5	2	1	3	8	9	s_4
17	5	2	2	2	9	9	$-2s_4 - 6s_7 - 6s_5 - 6s_6 - 6s_{10} - 2s_8 - 6s_9 - 6s_2 - 3s_3 + 168$
17	5	2	3	1	10	9	s_4
17	5	2	4	0	11	9	s_8
16	6	0	0	6	6	12	$-6s_{10} - s_4/3 - s_9 - s_8/3 + 21 - s_6 - s_2 - s_7$
16	6	0	1	5	7	12	$14 + 3s_7 + 2s_6 + s_4/3 - 2s_{10} - s_3 - 2s_8/3 - s_5 - 7s_9$
⋮					⋮		⋮

次に実際に符号の元を使って小関多項式を決定します。

(3) 整数 K に対して、目的の符号の部分集合 $C_{\leq K} := \{c \in C \mid \mathrm{wt}(c) \leq K\}$ を考える。適当な K に対して $O(a, C_{\leq K}; x, y, u, v, w)$ を (計算機等を用いて) 計算すれば (2) で残ったパラメータの値が決定されるので小関多項式が計算できる。もちろん K の値は出来るだけ小さいほうが計算は楽になる。

例えば $\mathrm{wt}(a) = 6$ の場合には、上の表を見て $K = 9$ ととればパラメータ $s_2, \ldots, s_{10}$ が計算できます。今までの方法 (補題 1 (2)) だと $P_a(C) = \{c \in C \mid \mathrm{wt}(c) < \mathrm{wt}(a) + D(C)\} = C_{\leq 13} = \{c \in C \mid \mathrm{wt}(c) \in \{0, 9, 12\}\}$ (80809 個) を用いてコセット重み枚挙多項式を計算しなければなりませんでしたが、上記の方法だと $\{c \in C \mid \mathrm{wt}(c) \in \{0, 9\}\}$(2185 個) を用いれば計算できることが分かります。このようなことは任意の符号、任意の重みに対して成立するわけではありません (例えば長さ 24 に対してはどちらの方法でも必要な K の値は変わらない)。しかし補題 1 (2) に対応する結果

(*) $O(a, C; x, y, u, v, w)$ の y, u, v に関する次数で $D(C) - 1$ 次までの係数が分かれば $O(a, C; x, y, u, v, w)$ は計算出来る。

は成り立つので、少なくとも今までの方法に較べて使用する K の値は大きくはならないことは分かります。

上の計算 (1)-(3) を全ての i $(0 \leq i \leq 7)$ と $a \in \mathbb{F}_3^{28}$ $(\mathrm{wt}(a) \leq i)$ に対して行います (実際は $i \leq 6$ までで良い)。この結果から実際に現れるコセット重み枚挙多項式と、それをコセット重み枚挙多項式としてもつコセットの数が次のように勘定出来ます。

(4) 計算できた小関多項式を見て、y, v, w に関する最低の次数が $\mathrm{wt}(a)$ より小さくなった場合は a は $a + C$ のコセットリーダではないのでその a は数えない。

(5) a をコセットリーダとする。$O(a, C; 1, x, x, x, 1)$ で $a + C$ のコセット重み枚挙多項式が計算できる。コセット重み枚挙多項式 $f(x)$ に対して

$$\frac{|\{a \text{ はコセットリーダ } \mid O(a, C; 1, x, x, x, 1) = f(x)\}|}{(f(x) \text{ の最低次の係数})}$$

が $f(x)$ をコセット重み枚挙多項式としてもつコセットの数となる。

計算した長さ 28 の符号のコセット重み分布 (= コセット重み枚挙多項式) を載せておきます。表の最後の行の数はそのようなコセット重み分布を持つコセットの数です。

コセット重み分布：長さ 28.

重み	0	1	2	7
0	1	0	0	0
1	0	1	0	0
2	0	0	1	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	52	36
8	0	351	104	189
9	2184	351	546	756
10	0	1482	3926	2772
11	0	16848	7852	9072
12	78624	16848	23400	26082
13	0	44928	73308	64260
14	0	205740	131640	137700
15	768096	205740	251460	256284
16	0	356616	416689	416619
17	0	694278	595634	588168
18	2159976	694278	732849	719712
19	0	771420	730340	757260
20	0	583362	689260	681534
21	1555632	583362	518544	518724
22	0	388908	341952	330372
23	0	92664	165360	172368
24	216216	92664	66924	72009
25	0	30888	27976	22932
26	0	1080	4472	5292
27	2240	1080	600	756
28	0	80	80	72
#	1	56	1512	40040

コセット重み分布：長さ 28.

重み	3	4
0	0	0
1	0	0
2	0	0
3	1	0
4	0	1
5	0	t_2
6	t	t_1
7	$-t+28$	$-t_1+2t_2+28$
8	$-3t+156$	$-3t_1-13t_2+207$
9	$-t+902$	$-15t_2-t_1+720$
10	$4t+2579$	$34t_2+4t_1+2710$
11	$8703+18t$	$9288+18t_1+30t_2$
12	$27418-15t$	$26055+63t_2-15t_1$
13	$-3t+63642$	$-3t_1-192t_2+64420$
14	$-45t+137610$	$-45t_1+10t_2+136836$
15	$253662+55t$	$-90t_2+256716+55t_1$
16	$418996-10t$	$416716-10t_1+380t_2$
17	$60t+590691$	$60t_1-115t_2+589104$
18	$718238-85t$	$30t_2+718974-85t_1$
19	$755885+25t$	$756736+25t_1-350t_2$
20	$-45t+678690$	$-45t_1+159t_2+681480$
21	$523300+69t$	$519156+45t_2+69t_1$
22	$329478-24t$	$330832-24t_1+138t_2$
23	$172890+18t$	$171936+18t_1-92t_2$
24	$70203-29t$	$-45t_2+71982-29t_1$
25	$23641+11t$	$22816+11t_1-4t_2$
26	$-3t+5583$	$20t_2-3t_1+5472$
27	$599+5t$	$720+12t_2+5t_1$
28	$74-2t$	$64-8t_2-2t_1$

コセット重み分布：長さ 28.

重み	5	6
0	0	0
1	0	0
2	0	0
3	0	0
4	0	0
5	t_1	0
6	t_2	t
7	$2t_1 - t_2 + 36$	$-t + 36$
8	$-3t_2 - 13t_1 + 189$	$-3t + 189$
9	$-15t_1 - t_2 + 756$	$-t + 756$
10	$4t_2 + 34t_1 + 2772$	$4t + 2772$
11	$9072 + 18t_2 + 30t_1$	$9072 + 18t$
12	$26082 - 15t_2 + 63t_1$	$26082 - 15t$
13	$-3t_2 + 64260 - 192t_1$	$64260 - 3t$
14	$-45t_2 + 137700 + 10t_1$	$137700 - 45t$
15	$256284 + 55t_2 - 90t_1$	$256284 + 55t$
16	$416619 - 10t_2 + 380t_1$	$416619 - 10t$
17	$60t_2 + 588168 - 115t_1$	$588168 + 60t$
18	$719712 - 85t_2 + 30t_1$	$719712 - 85t$
19	$757260 + 25t_2 - 350t_1$	$757260 + 25t$
20	$-45t_2 + 159t_1 + 681534$	$-45t + 681534$
21	$69t_2 + 518724 + 45t_1$	$518724 + 69t$
22	$330372 - 24t_2 + 138t_1$	$330372 - 24t$
23	$172368 + 18t_2 - 92t_1$	$172368 + 18t$
24	$72009 - 29t_2 - 45t_1$	$72009 - 29t$
25	$22932 + 11t_2 - 4t_1$	$22932 + 11t$
26	$-3t_2 + 5292 + 20t_1$	$5292 - 3t$
27	$756 + 5t_2 + 12t_1$	$756 + 5t$
28	$72 - 8t_1 - 2t_2$	$72 - 2t$

パラメータの値

重み 3	t	6	10		
	#	19656	6552		
4	(t_1,t_2)	(0,0)	(0,1)	(2,2)	(2,1)
	#	13104	39312	58968	58968
	(t_1,t_2)	(4,0)	(6,0)	(6,1)	
	#	39312	58968	58968	
5	(t_1,t_2)	(1,0)	(1,1)	(1,3)	(1,4)
	#	39312	39312	294840	432432
	(t_1,t_2)	(1,5)	(1,6)	(1,7)	(1,9)
	#	294840	393120	235872	58968
	(t_1,t_2)	(1,11)	(2,0)	(2,1)	(2,2)
	#	58968	19656	117936	58968
	(t_1,t_2)	(2,3)	(2,4)	(2,7)	(3,3)
	#	19656	117936	58968	39312
	(t_1,t_2)	(3,4)			
	#	39312			
6	t	2	3	4	5
	#	176904	275184	275184	412776
	t	6	7	8	9
	#	117936	235872	176904	236600
	t	10	11	14	15
	#	58968	78624	2808	19656
	t	27			
	#	728			

参考文献

[1] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, *Inform. Contr.* **23** (1973), 407–438.

[2] M. Harada, M. Ozeki, and K. Tanabe On the Covering Radius of Ternary Extremal Self-Dual Codes, preprint.

[3] W.C. Huffman, On extremal self-dual ternary codes of lengths 28 to 40, *IEEE Trans. Inform. Theory* **38** (1992), 1395–1400.

[4] M. Ozeki, On the notion of Jacobi polynomials for codes, *Math. Proc. Cambridge Philos. Soc.* Vol. 121 (1997), 15–30.

[5] M. Ozeki, On the covering radius problems for ternary self-dual codes, *Theoretical Comput. Sci.*, (to appear).

[6] K. Tanabe, Modified Jacobi polynomials of ternary codes and the invariant ring of a related group, preprint.