数理解析研究所講究録
第1752巻 2011年 22-26

量子符号に関係した古典符号

山形大学・理学部 原田 昌晃 (Masaaki Harada)
Faculty of Science, Yamagata University

1 はじめに

この原稿は, 京都大学数理解析研究所で行なわれた研究集会「諸分野との協働による数理科学のフロンティア」における講演内容をまとめたものである. 講演では, 量子符号に関係した古典符号についての紹介を, 著者の結果を少しだけ交えながら行なった. 講演時間が20分と限られたものであったためにそれほど深い内容については扱うことが出来なかったことをお許し願う.

まず, $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ で位数4の有限体を表すことにする, ただし $\omega^2 = \omega + 1$ である. $\mathbb{F}_4$ 上の長さ n, 次元 k の code とは $\mathbb{F}_4^n$ の k 次元部分空間のことである. C の dual code $C^\perp$ を $\{x \in \mathbb{F}_4^n \mid x \cdot y = 0 \ (\forall y \in C)\}$ で定義する, ただし $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_4^n$ に対して $x \cdot y = \sum_{i=1}^n x_i y_i^2$ とする. $C = C^\perp$ $(C \subset C^\perp)$ であるとき C を self-dual (self-orthogonal) とよぶ. $x = (x_1, \ldots, x_n) \in \mathbb{F}_4^n$ の weight $\mathrm{wt}(x)$ を $|\{i \mid x_i \neq 0\}|$ とする. C の minimum weight を $\min\{\mathrm{wt}(x) \mid \mathbf{0} \neq x \in C\}$ で定義し $d(C)$ で表す, ただし $\mathbf{0}$ はゼロベクトルを表す.

タイトルにある「古典」は「量子」への対比で使っており「古典符号」はここで定義した code を意味する. 著者の基本的な関心の一つは (self-dual) code をある組合せ構造とみて, (色々な意味において) 良い code の構成と分類を行なうことである.

2 Extremal self-dual code と self-dual code の分類

2.1 Extremal self-dual code

まず $\mathbb{F}_4$ 上の self-dual code C の weight enumerator を調べることで minimum weight に関する評価が与えられることについての説明をする. 長さ n の code C の weight enumerator とは $\mathbb{C}$ 上の2変数の多項式 $W_C(x, y) = \sum_{c \in C} x^{n - \mathrm{wt}(c)} y^{\mathrm{wt}(c)}$ のことである. C を長さ n の self-dual code[1] とすると

$$W_C(x, y) = W_C\Big(\frac{x + 3y}{2}, \frac{x - y}{2}\Big), \ W_C(x, y) = W_C(x, -y)$$

[1] 自動的に次元は $n/2$ となる.

が成り立つことが分かる. 前者は MacWilliams 恒等式から, 後者は $\mathrm{wt}(c) \in 2\mathbb{Z}$ $(\forall c \in C)$ である[2]ことから得られる. したがって

$$\frac{1}{2}\begin{pmatrix} 1 & 3 \\ 1 & -1 \end{pmatrix} \circ W_C(x,y) = W_C(x,y), \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \circ W_C(x,y) = W_C(x,y),$$

が成り立つ, ここで, 行列 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ と多項式 $f(x,y)$ に対して $A \circ f(x,y) = f(ax+by, cx+dy)$ とする. この 2 つの行列で生成される群

$$G = \left\langle \frac{1}{2}\begin{pmatrix} 1 & 3 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \ (\subset GL(2,\mathbb{C}))$$

を考えると $W_C(x,y)$ は G によって不変な多項式全体

$$\mathbb{C}[x,y]^G = \{f(x,y) \in \mathbb{C}[x,y] \mid A \circ f(x,y) = f(x,y) \ (\forall A \in G)\}$$

に含まれる. さらに, 次の結果が成り立つ

$$W_C(x,y) \in \mathbb{C}[x,y]^G = \mathbb{C}[x^2+3y^2, y^2(x^2-y^2)^2]$$

(MacWilliams–Mallows–Sloane [8]). この結果より $\mathbb{F}_4$ 上の self-dual code が存在するためにはその長さ n は偶数でなければいけないことが直ちに分かる. さらに

$$d(C) \leq 2\left\lfloor \frac{n}{6} \right\rfloor + 2 \tag{1}$$

が成り立つ (MacWilliams–Odlyzko–Sloane–Ward [9]).

以上から minimum weight に関する一つの評価が得られたので, 最良な場合を extremal とよぶ, つまり, $\mathbb{F}_4$ 上の長さ n の self-dual code C が $d(C) = 2\lfloor n/6 \rfloor + 2$ を満たすときに extremal とよび, その存在性については古くから調べられている. (1) は weight enumerator を考えることで代数的に得られた上限であるので, 著者の個人的な感想ではあるが, 最適であって欲しいが, 残念ながら長さ 12, 24, 26 では extremal self-dual code は存在しないことが知られている ([7], [9], [10] を参照). なお, extremal self-dual code の存在が分かっていない最小の長さは 32 である.

2.2 Self-dual code の分類

次に extremal だけなく $\mathbb{F}_4$ 上の self-dual code 全体の分類について考えていく. 2 つの $\mathbb{F}_4$ 上の self-dual code C, C' に対して, $C' = CM$ $(= \{cM \mid c \in C\})$ となる $\mathbb{F}_4$ 上の monomial matrix M が存在するときに C と C' は同値とよぶ[3]. この同値

[2] even code とよばれる.

[3] この定義は [9] に従う. 別の定義を採用している文献もある.

のもとで分類を行なう. さらに $C = CM$ となる monomial matrix M 全体を C の自己同型群とよび, $\mathrm{Aut}(C)$ と表す. 実際の分類は長さを固定して行なわれる訳であるが, 長さ n の全ての self-dual code を求めて同値判定をするというのが最も単純な方法である. しかしながら, 計算量が多くなりこれを避けるために役立つ結果が, 次の mass formula とよばれる等式である. 長さ n の互いに非同値な self-dual code 全体の集合を $\mathcal{C}_n$ で表すと

$$\prod_{i=0}^{n/2-1}(2^{2i+1}+1) = \sum_{C\in\mathcal{C}_n}\frac{n!3^n}{\#\,\mathrm{Aut}(C)} \tag{2}$$

が成り立つ (MacWilliams–Mallows–Sloane [8]). $\frac{n!3^n}{\#\,\mathrm{Aut}(C)}$ は C と同値な self-dual code の個数を意味し, 左辺は長さ n の self-dual code 全体の個数であることから (2) が成り立つことが分かる. したがって, 非同値である self-dual code を次々求めていき, $\frac{n!3^n}{\#\,\mathrm{Aut}(C)}$ の和が (2) の左辺の値に一致したときが分類の完成を意味する. 全ての self-dual code を求める必要がないことを分かっていただけるはずである. このような結果は self-dual code を考える面白さの一つであると思われる.

長さ 16 までの分類は [3] と [9] で完成されている (長さ 18 と 20 においては extremal self-dual code についてのみ [6] で分類が行なわれている). [3] と [9] は 1970 年代の結果であり, self-dual code の分類は基本的な問題であるが, その後, 進められていなかった. 今回, 長さ 18 と 20 の self-dual code の分類と長さ 22 の extremal self-dual code の分類を完成することが出来た (詳細は [4] と [5] をご覧いただきたい).

Proposition 1 (Harada–Lam–Munemasa–Tonchev [4], Harada–Munemasa [5]). 長さ 18 では 245 個の非同値な self-dual code が存在する. 長さ 20 では 3427 個の非同値な self-dual code が存在する. 長さ 22 では 723 個の非同値な extremal self-dual code が存在する.

表 1: Self-dual code の分類結果

n	$\#(n)$	文献	$\#_{\mathrm{E}}(n)$	文献	n	$\#(n)$	文献	$\#_{\mathrm{E}}(n)$	文献
2	1	[9]	1	[9]	14	21	[9]	1	[9]
4	1	[9]	1	[9]	16	55	[3]	4	[3]
6	2	[9]	1	[9]	18	245	[4]	1	[6]
8	3	[9]	1	[9]	20	3427	[5]	2	[6]
10	5	[9]	2	[9]	22	?		723	[5]
12	10	[9]	0	[9]	24	?		0	[10]

表 1 に self-dual code の分類結果をまとめる. $\#(n)$ は長さ n の非同値な self-dual code の個数を, $\#_{\mathrm{E}}(n)$ は長さ n の非同値な extremal self-dual code の個数を与える. また, それぞれの分類を完成させた文献も与える.

3 $\mathbb{F}_4$ 上の additive code と quantum code

前節で扱った $\mathbb{F}_4$ 上の self-dual code はそれ自体古くから活発な研究が行なわれている対象であり, [4] と [5] では長さ 18 と 20 の self-dual code の分類と長さ 22 の extremal self-dual code の分類を完成させた訳であるが, quantum code についての関連もありこの視点での興味もあった. 残りでは, quantum code についての関連についての説明をしたい.

今まで扱っていた code は $\mathbb{F}_4^n$ の k 次元部分空間であったが, 新たに additive code というものを考える. この節では, 今まで扱っていた code を additive と区別するために linear code とよぶことにする. $\mathbb{F}_4$ 上の additive $(n, 2^k)$ code C とは $\#C = 2^k$ となる $\mathbb{F}_4^n$ の加法部分群のことである. C の trace dual code C^* を $\{x \in \mathbb{F}_4^n \mid x * y = 0\ (\forall y \in C)\}$ で定義する, ただし $x * y = \mathrm{Tr}(x \cdot y)$ $(x, y \in \mathbb{F}_4^n)$ でこれは trace inner product とよばれる. $C = C^*$ $(C \subset C^*)$ であるとき C を trace self-dual (trace self-orthogonal) とよぶ.

C を linear code とすると, C が self-orthogonal であることと C が trace self-orthogonal であることは同値であることが簡単に分かる. したがって, 前節で扱った linear code で self-dual (self-orthogonal) であるものは additive code で trace self-dual (self-orthogonal) であるものの特別な場合であることが分かる.

$\mathbb{F}_4$ 上の additive trace self-orthogonal code の研究の動機としては, 次の基本的でかつ重要な結果が挙げられる[4].

Theorem 2 (Calderbank–Rains–Shor–Sloane [2]). C を $\mathbb{F}_4$ 上の additive trace self-orthogonal $(n, 2^{n-k})$ code とする $(1 \leq k)$. $C^* \setminus C$ の minimum weight が d である場合[5], C は quantum (stabilizer) $[[n, k, d]]$ code を与える. minimum weight d の additive trace self-dual $(n, 2^n)$ code は quantum (stabilizer) $[[n, 0, d]]$ code を与える.

現在, 色々な立場での quantum code の研究が行なわれている (例えば, この講究録の萩原学氏の原稿を参照). 古典符号と同じように quantum $[[n, k, d]]$ code に対しても, n と k を固定したときに最大となる d の値 ($d_{max}(n, k)$ で表す) を決定する研究が行なわれている. 次のデータベース

`http://www.codetables.de/`

に $k \leq n \leq 128$ についての $d_{max}(n, k)$ が記録されている. 上記のデータベースにおける最小の未解決のパラメーター[6]は $(n, k) = (13, 5)$ である. しかし $d_{max}(13, 5) = 3$ であることが [1] で示されていることを新谷誠氏より教えていただいた. したがって最小の未解決のパラメーターは $(n, k) = (14, 3)$ で $d_{max}(14, 3)$ は 4 と 5 のどちらであるかが分かっていない.

[4]未定義の用語については [2] を参照していただくことにする.
[5]$C^* \setminus C$ には weight d の vector が存在し weight $< d$ の vector が存在しない場合.
[6]原稿執筆時における.

最後に, 大きな d をもつ quantum $[[n,k,d]]$ code の構成には Theorem 2 が役立つと思われ, 今までに $\mathbb{F}_4$ 上の linear self-dual (self-orthogonal) code で行なってきたこと (例えば前節で紹介した結果など) を additive code まで拡げることで, 今後, quantum $[[n,k,d]]$ code の研究を行なうことが考えられる. 色々な立場での quantum code の研究が行なわれているが, ここで述べたような枠組での quantum code の研究も必要ではないかと著者は思っている.

参考文献

[1] J. Bierbrauer, S. Marcugini and F. Pambianco, The non-existence of a [[13,5,4]] quantum stabilizer code, (ArXiv: cs.IT/0908.1348).

[2] R.A. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, Quantum error correction via codes over GF(4), *IEEE Trans. Inform. Theory* **44** (1998), 1369–1387.

[3] J.H. Conway, V. Pless and N.J.A. Sloane, Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16, *IEEE Trans. Inform. Theory* **25** (1979), 312–322.

[4] M. Harada, C. Lam, A. Munemasa and V.D. Tonchev, Classification of generalized Hadamard matrices $H(6,3)$ and quaternary Hermitian self-dual codes of length 18, *Electronic J. Combin.* **17** (2010), #R171 (14 pp.).

[5] M. Harada and A. Munemasa, Classification of quaternary Hermitian self-dual codes of length 20, *IEEE Trans. Inform. Theory*, (to appear).

[6] W.C. Huffman, Characterization of quaternary extremal codes of lengths 18 and 20, *IEEE Trans. Inform. Theory* **43** (1997), 1613–1616.

[7] C.W.H. Lam and V. Pless, There is no $(24,12,10)$ self-dual quaternary code, *IEEE Trans. Inform. Theory* **36** (1990), 1153–1156.

[8] F.J. MacWilliams, C.L. Mallows and N.J.A. Sloane, Generalizations of Gleason's theorem on weight enumerators of self-dual codes, *IEEE Trans. Inform. Theory* **18** (1972), 794–805.

[9] F.J. MacWilliams, A.M. Odlyzko, N.J.A. Sloane and H.N. Ward, Self-dual codes over $GF(4)$, *J. Combin. Theory Ser. A* **25** (1978), 288–318.

[10] P.R.J. Östergård, There exists no Hermitian self-dual quaternary $[26,13,10]_4$ code, *IEEE Trans. Inform. Theory* **50** (2004), 3316–3317.