Mass Formula for Codes

宗政昭弘
東北大学大学院情報科学研究科

2007 年 8 月 3 日

1 Introduction

Mass formula とは、例えば n 次元 even unimodular lattice の同値類にわたる和

$$\sum_{[L]} \frac{1}{|\operatorname{Aut} L|} \tag{1}$$

を n の式で与える公式をいう [3, p.409]。これの類似として、例えば長さ n の自己双対符号の同値類にわたる和

$$\sum_{[C]} \frac{1}{|\operatorname{Aut} C|} \tag{2}$$

を n の式で与える公式も mass formula ということがある。さらにその一般化として、$\frac{1}{|\operatorname{Aut} C|}$ の分子を 1 の代わりに C の不変量、例えば weight enumerator で置き換えたものも mass formula の一般化と考えることができる。Lattice の場合と code の場合で異なる点は、code の場合はすべての C に対して $\operatorname{Aut} C$ を含む有限群が存在するので、その位数を両辺にかけることができるが、lattice の場合はそれができないことにより上の式を変形することができないことである。例えば、$\operatorname{Aut} C$ は permutation automorphism を意味するとすれば（実際 binary code ではそうである）、$\operatorname{Aut} C$ は対称群 S_n の部分群であり、(2) に $|S_n|$ をかけると、

$$\sum_{[C]} |S_n : \operatorname{Aut} C| = \sum_{C} 1.$$

となる。ただし、右辺の和は code の同値類にわたる和ではなく、code 全体の集合をわたる和となる。つまり、code の mass formula は、ある性質を満たす code（あるいは部分群）の個数を与える公式のことである。

最も単純な公式は、elementary abelian p-group of order p^n における、order p^k の部分群の個数、言い換えれば $\mathbf{F}_p$ 上の長さ n の k 次元 code の個数は

$$\prod_{i=0}^{k-1} \frac{p^{n-i}-1}{p^{k-i}-1}$$

で与えられることはよく知られている [6, p.34]。また、n を偶数とし、$\mathbf{F}_2^n$ に通常の内積を入れた場合に、$C = C^{\perp}$ を満たす部分群、すなわち自己双対符号の個数は

$$\prod_{i=1}^{(n/2)-1} (2^i + 1)$$

で与えられることが知られている。この他にもいろいろなクラスの code に関してその個数の公式がある [5, p.183]。その多くの場合において、そのクラスに属する code 全体に可移に作用する群があるために、公式で与えられている値がその群におけるある部分群の指数になっている。一方、そうでない場合については、mass formula の証明には全く違った方法が必要になる。そのためか、例えば $\mathbf{Z}_4$ 上の self-dual code の mass formula が得られたのは、binary self-dual code の mass formula ができてから 30 年以上たってからである [4]。その後 $\mathbf{Z}_9$ 上の self-dual code の mass formula [1], さらに一般に $\mathbf{Z}_{p^2}$ 上の self-dual code の mass formula が得られている [2]。

本稿では $\mathbf{Z}_{p^2}$ 上の self-dual code の mass formula を、群の拡大とコホモロジーの立場から、見通しの良いアプローチを与える可能性を示したい。ただし、まだ完全な別証明が完成したわけではない。この研究は R.A.L. Betty との共同研究である。

2 群拡大の部分群

C を $\mathbf{Z}_{p^2}$ 上の長さ n の code とすると、C から 2 つの $\mathbf{F}_p$ 上の長さ n の code が得られる：

$$C_1 = \text{residue code} = C \bmod p,$$
$$C_2 = \text{torsion code} = \{x \in \mathbf{F}_p^n \mid ps(x) \in C\},$$

ただし、$s : \mathbf{F}_p^n \to \mathbf{Z}_{p^2}^n$ は完全系列

$$0 \to \mathbf{F}_p^n \to \mathbf{Z}_{p^2}^n \to \mathbf{F}_p^n \to 0 \tag{3}$$

の section である、つまり、$\pi : \mathbf{Z}_{p^2}^n \to \mathbf{F}_p^n$ を自然な写像とすると、$\pi \circ s = \mathrm{id}$ となる写像 s である。このとき、次のことが容易にわかる。

Proposition 1. $C = C^\perp$ ならば

$$C_1 \subset C_1^\perp = C_2 \tag{4}$$

上記 (3) における injection $\mathbf{F}_p^n \to \mathbf{Z}_{p^2}^n$ を ι と書くと、

$$C_2 = \iota^{-1}(C), \quad C_1 = \pi(C) \tag{5}$$

である。そこで、self-dual code の総数を求めるためには、$C_1 \subset C_1^\perp = C_2$ を満たす $\mathbf{F}_p$ 上の codes C_1, C_2 に対して、(5) を満たす self-dual codes C の総数を求めて、それを (C_1, C_2) に関して和をとれば良いことになる。実際、これが Gaborit [4] による方法でもある。本稿では、この方法をただ真似をするのではなく、(5) を満たす self-dual codes C の総数に構造的な意味があることに注意し、より見通しの良い証明と mass formula 自体の一般化を目指す手がかりとしたい。

以後、完全系列 (3) の section s を固定し、C_1, C_2 を $\mathbf{F}_p^n$ の部分群とする。$x, y \in \mathbf{F}_p^n$ に対して、$s(x+y) - s(x) - s(y) \in \mathrm{Ker}\,\pi = \mathrm{Im}\,\iota$ だから、$s(x+y) - s(x) - s(y) = \iota(a)$ となる $a \in \mathbf{F}_p^n$ が存在する。このとき、$f : C_1 \times C_1 \to \mathbf{F}_p^n / C_2$ を $f(x,y) = a + C_2$ で定めると、f は 2-cocycle すなわち、$f \in Z^2(C_1, \mathbf{F}_p^n / C_2)$ である。さらに、次が成り立つ。

Proposition 2. C_1, C_2 を $\mathbf{F}_p^n$ の部分群とすると、(5) を満たす $\mathbf{Z}_{p^2}^n$ の部分群 C が存在するための必要十分条件は $f \in B^2(C_1, \mathbf{F}_p^n / C_2)$ となることである。さらに、このときこのような C の個数は $|Z^1(C_1, \mathbf{Z}_p^n / C_2)| = |\mathrm{Hom}(C_1, \mathbf{Z}_p^n / C_2)|$ である。

上の Proposition では、self-duality は全く考慮されていないため、実際は任意の有限アーベル群の完全系列に関して成り立つ。本当に欲しいのは、C_1, C_2 が (4) をみたすとき、(5) をみたし、かつ self-dual な C の個数である。このような C の個数は、[2] によれば、$k = \dim C_1$ とすると $p^{k(k-1)/2}$ である。ここで、$|\mathrm{Hom}(C_1, \mathbf{Z}_p^n / C_2)| = p^{k^2}$ であることに注目すると、$\mathrm{Hom}(C_1, \mathbf{Z}_p^n / C_2)$ が k 次正方行列全体の空間とすれば、$p^{k(k-1)/2}$

はその中の交代行列の個数である。この仕組みを明らかにすることが、目標への第１歩であると考えている。

また、[1, 2, 4] によれば、C_1, C_2 が (4) を満たせば、(5) を満たす self-dual code C が必ず存在することがわかっている。このことは、標準的な $\mathbf{F}_p$ 上の generator matrix が $\mathbf{Z}_{p^2}$ 上に lift できる、ということを示すことによっている。しかし一方、この事実は Proposition 2 によれば、$f \in B^2(C_1, \mathbf{F}_p^n/C_2)$ が成り立っていることを意味している。(4) を満たす C_1, C_2 が与えられたとき、$f \in B^2(C_1, \mathbf{F}_p^n/C_2)$ を直接示す方法は思いつかなかった。もちろん、(4) から $H^2(C_1, \mathbf{F}_p^n/C_2) = 0$ が導けるのであれば、$f \in B^2(C_1, \mathbf{F}_p^n/C_2)$ は自明となるのだが。

参考文献

[1] J.M.P. Balmaceda, R.A.L. Betty and F.R. Nemenzo, On the number of distinct self-dual codes over $\mathbf{Z}_9$, Matimyás Mat. 26 (2003), 9–17.

[2] J.M.P. Balmaceda, R.A.L. Betty and F.R. Nemenzo, Mass formula for self-dual codes over $\mathbf{Z}_{p^2}$, Discrete Math., to appear.

[3] J.H. Conway and N.J.A. Sloane, "Sphere Packing, Lattices and Groups," 3rd ed., Springer-Verlag, New York, 1999.

[4] P. Gaborit, Mass formulas for self-dual codes over $\mathbf{Z}_4$ and $\mathbf{F}_q + u\mathbf{F}_q$ rings, IEEE Trans. Inform. Theory, 42 (1996), 1222–1228.

[5] E. Rains and N.J.A. Sloane, Self-dual codes, in Handbook of Coding Theory, V.S. Pless and W.C. Huffman, eds., Elsevier, Amsterdam, 1998, 177–294.

[6] 寺田至，原田耕一郎「群論」，岩波書店，1997.