数理解析研究所講究録
第2053巻 2017年 5-13

Characterization of lattice polytopes and family of subsets closed under symmetric difference

東谷　章弘（京都産業大学）
E-mail: ahigashi@cc.kyoto-su.ac.jp

概 要

私の主な研究テーマは「格子凸多面体の組合せ論」です。ある特別な性質を満たす格子凸多面体の分類を議論すると、“対称差で閉じた集合族” の分類に帰着出来ることが分かりました。本稿では、格子凸多面体論に関する基本的なことから始め、格子単体の分類がある有限群の分類に帰着出来ることを紹介し、さらに、ある特別な格子単体の分類が二元線形符号（つまり、対称差で閉じた集合族）の分類に帰着出来ることを紹介します。最後に、Greismer 符号と呼ばれる特殊な二元線形符号との関連についても触れます。

1　凸多面体に関する導入

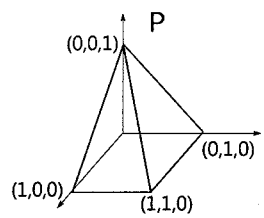
1.1　諸々の定義

$P \subset \mathbb{R}^d$ が**格子凸多面体**であるとは、頂点がすべて格子点（$\mathbb{Z}^d$ の点）であるような凸多面体のことである。より正確に述べると、有限個の $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{Z}^d$ が存在して $P = \mathrm{conv}(\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}) \subset \mathbb{R}^d$ と表せるときに言う。ただし $\mathrm{conv}(X)$ は集合 X の凸閉包を表す。

P° で P の内部を表す。格子凸多面体 $P \subset \mathbb{R}^d$ に対し、P の**次数**を

$$\deg(P) = \dim P + 1 - \min\{k : kP^\circ \cap \mathbb{Z}^d \neq \emptyset\}$$

で定義する。例えば、$P = \mathrm{conv}(\{(0,0,0),(1,0,0),(1,1,0),(0,1,0),(0,0,1)\})$（下記のような 3 次元格子凸多面体）とすると、$\deg(P) = 3 + 1 - 3 = 1$ となる。



d 次元格子凸多面体 $P \subset \mathbb{R}^d$ に対し、母函数 $\sum_{n\geq 0} |nP \cap \mathbb{Z}^d| t^n$ を考えると、有理関数の形になることが知られている：

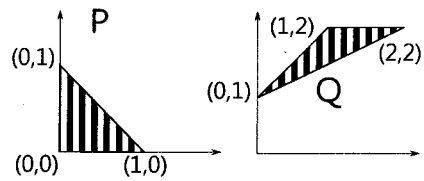
$$\sum_{n\geq 0} |nP \cap \mathbb{Z}^d| t^n = \frac{h_P^*(t)}{(1-t)^{d+1}}$$

(ただし $h_P^*(t)$ は t の多項式である。) P の次数 $\deg(P)$ は $h_P^*(t)$ の多項式としての次数に一致し、上記の $\deg(P)$ の定義はこれに由来する。

次に、格子凸多面体に対する "同値" を定義する。

- アフィン変換 $T : \mathbb{R}^d \to \mathbb{R}^d$ で $T(\mathbb{Z}^d) = \mathbb{Z}^d$ を満たすものを **unimodular 変換**という。これは、$M \in \mathrm{GL}_d(\mathbb{Z})$ と $\mathbf{u} \in \mathbb{Z}^d$ を用いて $T(\mathbf{x}) = M \cdot \mathbf{x} + \mathbf{u}$ $(\mathbf{x} \in \mathbb{R}^d)$ と表せる。
- 格子凸多面体 $P, Q \subset \mathbb{R}^d$ に対し、P と Q が **unimodular 同値**であるとは、unimodular 変換 T が存在して $Q = T(P)$ とできるときに言う。

例えば、下記の P と Q は unimodular 同値である。以下、格子凸多面体は unimodular 同値なものは同一視して考える。



もう一つ、unimodular 同値ではないが本質的に同じ格子凸多面体を構成する方法について述べる。

- 格子凸多面体 $P \subset \mathbb{R}^d$ に対し、P 上の**格子錐** $\mathrm{Pyr}(P)$ は

$$\mathrm{Pyr}(P) = \mathrm{conv}(\{(\alpha, 0) : \alpha \in P\} \cup \{(0, \ldots, 0, 1)\}) \subset \mathbb{R}^{d+1}$$

で定義する。このとき $\dim(\mathrm{Pyr}(P)) = \dim P + 1$ である。

格子凸多面体とその格子錐は unimodular 同値ではないが、前述の多項式 $h_P^*(t)$ と $h_{\mathrm{Pyr}(P)}^*(t)$ が一致する。特に、$\deg(P) = \deg(\mathrm{Pyr}(P))$ である。

1.2 格子凸多面体論における研究動機

格子凸多面体論における研究の主な目的の 1 つは、格子凸多面体の構造を理解することである。このとき、格子凸多面体は unimodular 同値を除いて、かつ、格子錐の構造を除いて考える。より具体的な問題として、近年、下記の予想の解決が重要な課題の 1 つであると思われる。

予想 1 ([3, Conjecture 1.2]). P を次数 s の d 次元格子凸多面体とする。もし $d > 2s$ ならば、P は Cayley 分解を持つ。

Cayley 分解の詳細については割愛するが、格子錐の概念を一般化したようなものである。上記の予想は **Cayley 予想**と呼ばれ、近年盛んに研究されている。

一方で、次のような結果が知られている。

定理 2 ([7, Theorem 10], [6, Proposition 2.3]). Δ を次数 s の d 次元格子単体とする。もし Δ が格子錐の構造を持たないならば、$d + 1 \leq f(2s) \leq 4s - 1$ を満たす。

ただし、正の整数 m に対し、

$$f(m) = \sum_{\ell=0}^{\infty} \left\lfloor \frac{m}{2^\ell} \right\rfloor$$

とする。この定理は $d \geq f(2s)$ ならば Δ が常に格子錐の構造を持つことを示している。この定理は [7] において $d+1 \leq 4s-1$ という不等式が示されているが、その証明を修正することで [6] において $d+1 \leq f(2s)$ という不等式に改善されている。また、[7, Theorem 7] で一般の格子凸多面体の場合も議論されている。

Cayley 予想は、次数に比べて次元が十分大きいと常に Cayley 分解を持つことを予想したものであり、定理 2 を精密化して一般化したものであると思える。Cayley 予想の解決に向けて、下記の問題に取り組むのは非常に自然である。

問題 3. 正の整数 s に対し、次数 s の $(f(s)-1)$ 次元格子単体で格子錐の構造を持たないものを特徴付けよ。

2 格子単体と二元線形符号の関係

問題 3 に取り組むに当たり、まず、[1, Section 2] で言及されている対応を導入する。つまり、格子単体とある有限アーベル群が対応することについて紹介する。さらに、考察したい格子単体がある二元線型符号と対応することについて紹介する。

2.1 格子単体と有限アーベル群と線型符号

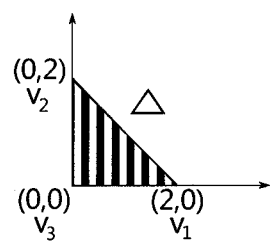
$\Delta \subset \mathbb{R}^d$ を格子単体とし、$\mathbf{v}_1, \ldots, \mathbf{v}_{d+1} \in \mathbb{Z}^d$ を Δ の頂点とする。集合 Λ_Δ を次のようにして定義する：

$$\Lambda_\Delta = \left\{ (x_1, \ldots, x_{d+1}) \in (\mathbb{R}/\mathbb{Z})^{d+1} : \sum_{i=1}^{d+1} x_i \in \mathbb{Z}, \sum_{i=1}^{d+1} x_i \mathbf{v}_i \in \mathbb{Z}^d \right\}$$

例 4. 例えば、$\Delta = \mathrm{conv}(\{(0,0),(2,0),(0,2)\})$（下記のような 2 次元格子単体）とすると、

$$\Lambda_\Delta = \{(0,0,0),(1/2,1/2,0),(1/2,0,1/2),(0,1/2,1/2)\}$$

となる。



集合 Λ_Δ は有限アーベル群をなすことがわかる。例えば例 4 は、群として $(\mathbb{Z}/2\mathbb{Z})^2$ と同型である。

有限アーベル群 Λ_Δ は Δ の性質を大きく反映している。例えば、以下が成り立つことが知られている。

$$(\Delta \text{の体積}) \cdot d! = (\Lambda_\Delta \text{の位数})$$

$$\deg(\Delta) = \max\left\{\sum_{i=1}^{d+1} x_i : (x_1, \ldots, x_{d+1}) \in \Lambda_\Delta, 0 \leq x_i < 1\right\}$$

$$\Delta \text{が格子錐でない} \Leftrightarrow 1 \leq \forall i \leq d+1,\ \exists (x_1, \ldots, x_{d+1}) \in \Lambda_\Delta \text{ s.t. } x_i \neq 0$$

また、[1, Theorem 2.3] において、次のような 1 対 1 対応が知られている：

$$\{d \text{次元格子単体}\}/(\text{unimodular 同値}) \longleftrightarrow$$
$$\{\text{有限アーベル部分群 } \Lambda \subset (\mathbb{R}/\mathbb{Z})^{d+1} \text{ で成分和が常に整数}\}/(\text{座標の入れ替え})$$

例 4 について再考する。Λ_Δ における $1/2 \in \mathbb{R}/\mathbb{Z}$ を $1 \in \mathbb{Z}/2\mathbb{Z}$ と同一視すると、Λ_Δ は $(1,1,0), (1,0,1) \in (\mathbb{Z}/2\mathbb{Z})^3$ を基底とする $\mathbb{Z}/2\mathbb{Z}$ 上の線型空間、つまり（二元）線型符号と見なすことができる。

この対応は一般の Λ_Δ に拡張することができる。逆に、正の整数 n に対し、線型符号 $C \subset (\mathbb{Z}/n\mathbb{Z})^{d+1}$ で

$$\text{任意のベクトルの成分和が } n \text{ の倍数} \cdots\cdots (*)$$

を満たすものに対して、有限アーベル部分群 $\Lambda \subset (\mathbb{R}/\mathbb{Z})^{d+1}$ で成分和が常に整数になるものを対応させることができる。

したがって、次のような 1 対 1 対応を得ることができる。

$$\{d \text{次元格子単体}\}/(\text{unimodular 同値}) \longleftrightarrow \tag{2.1}$$
$$\{\text{線型符号 } C \subset (\mathbb{Z}/n\mathbb{Z})^{d+1} \text{ で } (*) \text{ を満たすもの}\}/(\text{座標の入れ替え})$$

2.2 二元シンプレックス符号

本稿において本質的な役割を担う「二元シンプレックス符号」を導入する。

行列 $H(r) \in (\mathbb{Z}/2\mathbb{Z})^{r \times (2^r - 1)}$ は、$\mathbf{0}$ 以外のすべての $(0,1)$-ベクトルを列ベクトルに持つ行列とする。例えば、

$$H(2) = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad H(3) = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

となる。r **次元二元シンプレックス符号** $C \subset (\mathbb{Z}/2\mathbb{Z})^r$ とは、行列 $H(r)$ の行ベクトルで生成された二元線形符号のことである。二元シンプレックス符号はハミング符号の双対符号でもある。

正の整数 r に対し、r 次元二元シンプレックス符号は $(2^r-1, r, 2^{r-1})$ 符号（符号長 2^r-1、r 次元、最小重み 2^{r-1}）であり、一定重み符号（つまり $\mathbf{0}$ 以外のハミング重みが 2^{r-1} で一定）であることが知られている。したがって、条件 $(*)$ を満たすことが分かる。よって、上記で説明した同一視 (2.1) を経由して得られる格子単体が考えられる。

$\Delta(r)$ を r 次元二元シンプレックス符号に付随する格子単体とする。二元シンプレックス符号の性質から $\dim(\Delta(r+2))+1 = 2^{r+2}-1 = 4\cdot 2^r - 1$ かつ $\deg(\Delta(r+2)) = 2^r$ を満たすことが分かる。つまり、定理2における不等式 $d+1 \leq 4s-1$ の等式を満たすことが分かる。

実は、この逆も成立する。

定理 5. Δ を次数 s の d 次元格子単体で格子錐の構造を持たないとする。もし $d+1 = 4s-1$ を満たすならば、ある $r \in \mathbb{Z}_{\geq 0}$ が存在して $s = 2^r$ となり、Δ は $\Delta(r+2)$ と unimodular 同値になる。

例えば、例4の格子単体は $\Delta(2)$ と unimodular 同値である。実際、例4の格子単体は次数1の2次元格子単体である。

さらに、一般に $d+1 = f(2s)$ を満たす格子単体に対しては以下が成り立つことが分かる。

定理 6. Δ を次数 s の d 次元格子単体で格子錐の構造を持たないとする。もし $d+1 = f(2s)$ を満たすならば、Δ はある二元符号を用いて表すことができる。より正確に述べると、$\Lambda_\Delta \subset \{0, 1/2\}^{d+1}$ が成り立つ。

3 格子凸多面体の特徴付けと対称差で閉じた集合族

本章は柏原賢二氏（東京大学）との共同研究に基づく。

定理6により、問題3はある特別な性質を満たす二元符号の問題に完全に帰着された。二元符号は「対称差で閉じた集合族」と同値である。以下、対称差で閉じた集合族の言葉で問題3に取り組む。

まず、記号を用意する。

- 正の整数 n に対し、$[n] := \{1, 2, \ldots, n\}$ とする。
- 集合 A, B に対し、A と B の**対称差** $A \triangle B$ は $A \triangle B = (A \cup B) \setminus (A \cap B)$ で定義される。
- 集合族 $\mathcal{A}$ が**対称差で閉じている**とは、任意の $A, B \in \mathcal{A}$ に対して $A \triangle B \in \mathcal{A}$ となるときに言う。以下、本稿で「集合族」といえば常に「対称差で閉じた集合族」を意味する。
- 集合族 $\mathcal{A}$ が集合 $A_1, \ldots, A_k$ で**生成される**とは、任意の集合 $A \in \mathcal{A}$ が $A = A_{i_1} \triangle \cdots \triangle A_{i_\ell}$（ただし $1 \leq i_1 < \cdots < i_\ell \leq k$）とできる時に言い、$A_1, \ldots, A_k$ で生成されている集合族を $\langle A_1, \ldots, A_k \rangle$ で表す。
- 集合族 $\mathcal{A}$ に対し、$\bigcup_{A \in \mathcal{A}} A = X$ なる X を $\mathcal{A}$ の**土台集合**と呼ぶ。
- 集合族 $\mathcal{A}, \mathcal{B}$ の土台集合をそれぞれ X, Y とする。$\mathcal{A}$ と $\mathcal{B}$ が**同型**であるとは、X と Y の間に全単射 σ が存在して σ が $\mathcal{A}$ と $\mathcal{B}$ の間の全単射を誘導する時に言う。

- 以下、$[r]$ の部分集合 $A \subset [r]$ と $(\epsilon_i)_{1\leq i\leq r} \in \{0,1\}^r$ という $(0,1)$-ベクトルとの同一視を多用する。ただし、

$$\epsilon_i = \begin{cases} 1 & (i \in A) \\ 0 & (i \notin A) \end{cases}$$

である。

二元符号 $C \subset (\mathbb{Z}/2\mathbb{Z})^r$ と $[r]$ の部分集合族は

$$(a_1,\dots,a_r) \in (\mathbb{Z}/2\mathbb{Z})^r \leftrightarrow \{i \in [r] : a_i = 1\}, \quad \mathbf{x}+\mathbf{y}\ (\mathbf{x},\mathbf{y} \in C) \leftrightarrow A \triangle B\ (A,B \in \mathcal{A})$$

という対応を用いて自然に同一視できる。これを通して、定理2は集合族の言葉で以下のように言い換えることができる。

命題 7. 正の整数 r と m に対し、土台集合が $[r]$ である集合族 $\mathcal{A}$ で $\max_{A\in\mathcal{A}} |A| = m$ を満たすとする。このとき、$r \leq f(m) \leq 2m-1$ が成立する。

注 8. 「d 次元で格子錐の構造を持たない」＝「土台集合が $[d+1]$ である」、「次数 s」＝「$\max_{A\in\mathcal{A}} |A| = 2s$」という言い換えを適用している。

したがって、問題3も次のように言い換えることができる。

問題 9. 正の整数 m に対し、土台集合が $[f(m)]$ である集合族 $\mathcal{A}$ で $\max_{A\in\mathcal{A}} |A| = m$ を満たすものを特徴付けよ。

さらに、定理5は以下のように言い換えることができる。

定理 10 (定理5の言い換え). 正の整数 m に対し、$\mathcal{A}$ は土台集合が $[2m-1]$ である集合族で $\max_{A\in\mathcal{A}} |A| = m$ を満たすものとする。この時、ある非負整数 r で $m = 2^r$ とでき、かつ、$\mathcal{A}$ は $H(r+1)$ の行ベクトルに対応する $[2m-1]$ の部分集合で生成された集合族と同型になる。

例えば、$H(3) = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$ であるので、各行ベクトルは $\{1,\dots,7\}$ の部分集合 $1235, 1246, 1347$ に対応する。（$\{i_1,\dots,i_\ell\}$ を $i_1\cdots i_\ell$ と略記している。）よって $r=2$ の場合は

$$\langle 1235, 1246, 1347\rangle = \{\emptyset, 1235, 1246, 1347, 3456, 2457, 2367, 1567\}$$

という集合族が対応する。

ここで、$f(m)$ について考える。以下の命題が簡単に示せる。

命題 11. 正の整数 m の二進展開を $m = 2^{u_1} + \cdots + 2^{u_p}$ とする。ただし、$u_1 > \cdots > u_p \geq 0$ とする。このとき、$f(m) = 2m - p$ が成り立つ。特に、$f(m) = 2m-1$ となる必要十分条件は m が2ベキとなることである。

m が2ベキの場合は定理10そのものであるので、以下、m が2ベキ以外の場合について考える。具体的には、まずは2つの非負整数 $r > r' \geq 0$ を用いて $m = 2^r + 2^{r'}$ とできる整数を考える。このとき命題11から、$f(m) = 2m-2$ である。

定理 12. 整数 $m = 2^r + 2^{r'}$ に対し、$\mathcal{A}$ は土台集合が $[2m-2]$ である集合族で $\max_{A\in\mathcal{A}} |A| = m$ を満たすものとする。この時、$\mathcal{A}$ は $H(r+1, r'+1, t)$ の行ベクトルに対応する $[2m-2]$ の部分集合で生成された集合族と同型になる。

ここで、3つの整数 $r > r' \geq t \geq 0$ に対し、$H(r, r', t)$ は $(r+t) \times (2^r + 2^{r'} - 2)$ 行列でその列ベクトルが $H(r)$ の列ベクトルに t 個 0 を下に加えたものと $H(s)$ の列ベクトルに $(r-s+t)$ 個 0 を 0 だけの行ベクトルがないように加えたものとする。例えば、

$$H(3,2,1) = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

となる。さらに、$H(r, 0, 0)$ は $H(r)$ と一致する。

また、一般の m に対しては、次のようなことが観察できる。

命題 13. 正の整数 m に対し、$\mathcal{A}$ は土台集合が $[f(m)]$ である集合族で $\max_{A\in\mathcal{A}} |A| = m$ を満たすものとする。また、$r = \lfloor \log_2 m \rfloor$ とおく。このとき、$\mathcal{A}$ は少なくとも $(r+1)$ 個の元で生成される。さらに、$\mathcal{A}$ の生成行列は $H(r+1)$ を部分行列に含む。

ここで、$\mathcal{A}$ の生成行列とは、$\mathcal{A}$ を生成する集合 $A_1, \ldots, A_k$ と同一視される $(0,1)$-ベクトルを行ベクトルに持つ $(0,1)$-行列のことである。

命題 14. 正の整数 m の二項展開を $m = 2^{u_1} + \cdots + 2^{u_p}$ とする。土台集合が $[f(m)]$ である集合族 $\mathcal{A}$ で $\max_{A\in\mathcal{A}} |A| = m$ を満たし、(u_1+1) 個の集合で生成されているものを考える。このとき、$\mathcal{A}$ が唯一つに決まる必要十分条件は $p = 1$ または $p = 2$ となるときである。

例 15. 以下の2つの集合族を考える。

$$\mathcal{A}_1 = \langle \{1,2,3,4,8,9,11\}, \{1,2,5,6,8,10\}, \{1,3,5,7\} \rangle,$$
$$\mathcal{A}_2 = \langle \{1,2,3,4,8,9\}, \{1,2,5,6,8,10\}, \{1,3,5,7,11\} \rangle$$

このとき、$\mathcal{A}_i$ はそれぞれ土台集合が $\{1, \ldots, 11\}$ である集合族で $\max_{A\in\mathcal{A}_i} |A| = 7$ を満たし、3つの集合で生成されている。$f(7) = 11$ であり $7 = 2^2 + 2^1 + 2^0$ であることに注意する。

一方、任意の $A \in \mathcal{A}_1$ に対して $|A| \neq 5$ であることがわかる。他方、$\{1,3,5,7,11\} \in \mathcal{A}_2$ である。したがって、$\mathcal{A}_1$ と $\mathcal{A}_2$ は明らかに同型ではない。これは $p = 3$ の時には、土台集合が $[f(m)]$ である集合族 $\mathcal{A}$ で $\max_{A\in\mathcal{A}} |A| = m$ を満たして (u_1+1) 個の集合で生成されているものが唯一つに決まらないことを示している。

4 Greismer 符号との関連

講演の際には紹介できなかったが、本稿の内容は Greismer 符号と呼ばれるものと密接に関連していることについて紹介する。

正の整数 k と d に対し、

$$g(k,d) = \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil$$

とおく。一方で、

$$n(k,d) = \min\{n : (n,k,d) \text{ 二元符号が存在する }\}$$

と定義する。1960 年に Greismer によって、

$$n(k,d) \geq g(k,d)$$

が成り立つことが証明された ([4])。この下限 $g(k,d)$ を **Greismer 下限**と呼び、$(g(k,d),k,d)$ 二元符号を **Greismer 符号**と呼ぶ。(Greismer 下限は二元符号とは限らない線型符号に対しても一般化されているが、本稿では二元符号のみ扱う。)

さらに、1973 年に Belov–Logachev–Sandimirov によって、以下がの命題が証明された。

命題 16 ([2]). 正の整数 k と d に対し、$t = \lceil d/2^{k-1} \rceil$ とおき、整数 $u_1, \ldots, u_p$ を $t > u_1 > \cdots > u_p \geq 1$ かつ $t \cdot 2^{k-1} - d = \sum_{i=1}^{p} 2^{u_i - 1}$ を満たすものとして定義する。このとき、$(g(k,d),k,d)$ 符号が存在するならば、$\sum_{i=1}^{\min\{p,t+1\}} u_i \leq tk$ を満たす、または、任意の $t \leq i \leq p-1$ で $u_{i+1} = u_i - 1$ かつ $u_p \in \{1,2\}$ を満たす。

さらに、1981 年、Helleseth によって、上記の記号の t が 1 の場合 (つまり $d \leq 2^{k-1}$) において $(g(k,d),k,d)$ 二元符号、つまり、Greismer 符号を完全に特徴付けた ([5])。

実は、第 3 章で議論した集合族はこの Greismer 符号と密接に関連している。具体的には、命題 16 の条件を満たす k,d で $t = 1$ なるものに対して、$(g(k,d),k,d)$ 符号から望む集合族を構成することができる。

以下、正の整数 k,d は $d \leq 2^{k-1}$ を満たすとし、整数 $u_1, \ldots, u_p$ で $k > u_1 > \cdots > u_p \geq 1$ を満たすもので $2^{k-1} - d = \sum_{i=1}^{p} 2^{u_i - 1}$ と書けるとする。さらに、条件

$$\sum_{i=1}^{\min(p,2)} u_i \leq k \text{ または 任意の } i = 1,2,\ldots,p-1 \text{ に対して } u_{i+1} = u_i - 1 \text{ かつ } u_p = 2$$

を満たすとする。

C を $(g(k,d),k,d)$ 符号とする。このとき、C の生成行列は同じ列ベクトルを 2 つ持たないことが知られている。そこで、C の**アンチ符号** C' を考える。ただし、C のアンチ符号とは、C の生成行列 M に対して $H(k) = (M|M')$ を満たすような行列 M' を生成行列に持つ二元符号のことである。例えば、生成行列 $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ をもつ二元符号 C は $(3,3,1)$ 符号であり、$g(3,1) = 3$ より、C は Greismer 符号である。一方で、C のアンチ符号 C' は生成行列 $\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$ を持つ二元符号のことである。このアンチ符号を集合族に置き換えると、$\mathcal{A} = \langle \{1,2,4\}, \{1,3\}, \{1,2,3\} \rangle$ となるが、このとき、$\mathcal{A}$ の土台集合は $\{1,2,3,4\}$ であり、かつ、$\max_{A \in \mathcal{A}} |A| = 3$ である。$f(3) = 4$ であるので、$\mathcal{A}$ は第 3 章で考察した集合族そのものである。

この構成方法は一般に行うことができる。もう少し正確に述べると、以下の命題が成り立つ。

命題 17. k, d を上記の条件を満たすとする。このとき、$(g(k,d), k, d)$ 符号に対し、土台集合 $[f(2^{k-1}-d)]$ 上の集合族 $\mathcal{A}(k,d)$ で $\max_{A\in\mathcal{A}(k,d)}|A| = 2^{k-1}-d$ なるものが存在する。

ただし、第3章で考察した集合族はいつでもこの方法で得られるわけではない。例えば、$\mathcal{A} = \langle\{1,2,4\},\{1,3\}\rangle$ とおくと、$\mathcal{A}$ は土台集合 $\{1,2,3,4\}$ 上の集合族であり $\max_{A\in\mathcal{A}}|A| = 3$ である。$f(3) = 4$ であるので、これは望む集合族である。一方で、上記の対応によってこの集合族を構成することは出来ない。

参考文献

[1] V.V. Batyrev and J. Hofscheier, Lattice polytopes, finite abelian subgroups in $\mathrm{SL}(n;\mathbb{C})$ and coding theory, arXiv:1309.5312, (2013).

[2] B. I. Belov, V. N. Logachev and V. P. Sandimirov, Construction of a class of linear binary codes achieving the Varshamov-Griesmer bound, *Prob. Inform. Transm.* 211-217. (1974).

[3] A. Dickenstein and B. Nill, A simple combinatorial criterion for projective toric manifolds with dual defect, *Math. Res. Lett.* **17** (3): 435–448, (2010).

[4] J. H. Griesmer. A bound for error-correcting codes, *IBM J. Res. Develop.* **4**: 532–542, (1960).

[5] T. Helleseth, A characterization of codes meeting the Griesmer bound, *Inform. and Control* **50** 128–159, (1981).

[6] A. Higashitani, Lattice simplices of maximal dimension with a given degree, arXiv:1605.00273.

[7] B. Nill, Lattice polytopes having h^*-polynomials with given degree and linear coefficient, *Eur. J. Comb.*, **29** (7): 1596–1602, (2008).