数理解析研究所講究録
第1564巻 2007年 131-137

A strengthening of the Assmus-Mattson theorem based on the displacement and split decompositions

東北大学・大学院情報科学研究科　田中 太初 (Hajime Tanaka)
Graduate School of Information Sciences,
Tohoku University

1 Introduction

代数的組合せ論の主要な研究対象である**アソシエーションスキーム**は有限可移置換群の満たす組合せ的性質を抽出したものと捉えられる。各アソシエーションスキームに対し中心化環に相当する **Bose-Mesner 代数**と呼ばれる代数が付随し、それが可換なときそのアソシエーションスキームを可換であると言う。Delsarte は 1973 年の記念碑的論文 [6] で符号及び組合せデザインの概念を任意の可換アソシエーションスキーム上に拡張し、Bose-Mesner 代数の性質や線型計画の手法を高度に駆使して符号・デザインに関する種々の優れた理論を展開した。Delsarte の理論は 1973 年の時点で既に実質的にはほぼ完成した理論だったと言っても過言ではないと思われるが、最近になって大きな進展が三つ立て続けに起こった。すなわち Brouwer, Godsil, Koolen, Martin [4] による **width・dual width** の理論、Terwilliger [16] による **displacement decomposition** の理論、及び Schrijver [10] による Terwilliger 代数を用いた半正定値計画の手法の確立である[1]。ここで **Terwilliger 代数**はアソシエーションスキームの構造の研究に於いて非常に有効な道具として Terwilliger [13, 14, 15] により導入された、各頂点に付随する非可換代数である。Bose-Mesner 代数は Terwilliger 代数の部分代数であり、群が作用する場合さらに Terwilliger 代数はその頂点の安定部分群の中心化環の部分代数である。これら三つの理論はいずれも Delsarte の理論に新たな息吹をもたらすことが期待されるものばかりであるが、本稿では特に [16] の結果の直接的な応用として、(線型) 符号と組合せデザインを結び付ける **Assmus-Mattson の定理**を取り上げる：

Theorem 1.1 (Assmus-Mattson [1]). *Let Y denote a linear code of length D over $\mathbb{F}_q$ with minimum weight δ. Let $Y^{\perp}$ denote the dual code of Y, with minimum weight δ^*. Suppose $t \in \{1,2,\ldots,D\}$ is such that there are at most $\delta - t$ weights of $Y^{\perp}$ in $\{1,2,\ldots,D-t\}$, or such that there are at most $\delta^* - t$ weights of Y in $\{1,2,\ldots,D-t\}$. Then the supports of the words of any fixed weight in Y form a t-design.*

2 Preliminaries

本稿では簡単のため通常の意味での符号を取り扱う枠組みである Hamming スキームのみを考察する。アソシエーションスキーム全般に関する基本的な文献としては、Bannai-Ito

[1] 半正定値計画 (semidefinite programming) は線型計画をより一般化したものである。簡潔にまとめた文献としては [17] がある。

[2] 及び Brouwer-Cohen-Neumaier [3] をご覧いただきたい。

まず語 $x=(x_1,x_2,\ldots,x_D)\in\mathbb{F}_q^D$ の **support** 及び **weight** をそれぞれ

$$\mathrm{supp}(x):=\{1\leqslant i\leqslant D : x_i\neq 0\},\quad \mathrm{wt}(x):=|\mathrm{supp}(x)|$$

とし、語 $x,y\in\mathbb{F}_q^D$ の **Hamming 距離**を $\partial(x,y):=\mathrm{wt}(x-y)$ により定める。ここでは集合 $\mathbb{F}_q^D$ とその上の Hamming 距離 $\partial(\cdot,\cdot)$ の組を **Hamming スキーム**と呼ぶことにし、$\mathrm{H}(D,q):=(\mathbb{F}_q^D,\partial(\cdot,\cdot))$ と書く。$\mathbb{F}_q^D$ 上には対称群 $\mathfrak{S}_q$ 及び $\mathfrak{S}_D$ の wreath 積 $G:=\mathfrak{S}_q\wr\mathfrak{S}_D$ が自然に作用するが、Hamming 距離 $\partial(\cdot,\cdot)$ は明らかに G の作用により不変である。

さて、$V:=\mathrm{Span}_{\mathbb{C}}\{\hat{x}:x\in\mathbb{F}_q^D\}$ を $\mathbb{F}_q^D$ で添え字付けられた基底を持つ複素数体上のベクトル空間とし、この基底に関して $\mathrm{End}_{\mathbb{C}}V$ を行・列がやはり $\mathbb{F}_q^D$ で添え字付けられた行列全体のなす代数とみなすことにする。$\mathrm{H}(D,q)$ の**隣接行列**[2] $A\in\mathrm{End}_{\mathbb{C}}V$ を

$$A_{xy}:=\begin{cases}1 & \text{if } \partial(x,y)=1\\ 0 & \text{otherwise}\end{cases}$$

と定めると、G の中心化環 $\mathrm{End}_{\mathbb{C}[G]}V$ が A により生成されることが容易に検証される[3]。別の言い方をすると、この場合 $\mathrm{H}(D,q)$ の **Bose-Mesner 代数**は $\mathrm{End}_{\mathbb{C}[G]}V$ に一致する。以後 Terwilliger の表記に従い $M:=\mathrm{End}_{\mathbb{C}[G]}V$ と書くことにする。M は $D+1$ 次元であり、実対称行列 A は $D+1$ 個の異なる実固有値 $\theta_0>\theta_1>\cdots>\theta_D$ を持つ[4]。各 $0\leqslant j\leqslant D$ に対し $E_j\in\mathrm{End}_{\mathbb{C}}V$ を j 番目の固有空間 $\{v\in V : Av=\theta_j v\}$ への直交射影とすると、$E_0,E_1,\ldots,E_D$ は半単純代数 M の原始冪等元の基底をなす。

次に各 $0\leqslant i\leqslant D$ に対し $E_i^*\in\mathrm{End}_{\mathbb{C}}V$ を i 番目の subconstituent $\mathrm{Span}_{\mathbb{C}}\{\hat{x}:\mathrm{wt}(x)=i\}$ への直交射影とする。すなわち E_i^* は次で定まる対角行列である：

$$(E_i^*)_{xx}=\begin{cases}1 & \text{if } \mathrm{wt}(x)=i\\ 0 & \text{otherwise}\end{cases}$$

このとき実はゼロ・ベクトル $\mathbf{0}:=(0,0,\ldots,0)\in\mathbb{F}_q^D$ の安定部分群 $H:=\mathrm{Stab}_G(\mathbf{0})\cong\mathfrak{S}_{q-1}\wr\mathfrak{S}_D$ の中心化環 $\mathrm{End}_{\mathbb{C}[H]}V$ は A 及び $E_0^*,E_1^*,\ldots,E_D^*$ により生成されることが証明される[5]。言い換えると、この場合 $\mathrm{H}(D,q)$ の（$\mathbf{0}$ に関する）**Terwilliger 代数** [13, 14, 15] は $\mathrm{End}_{\mathbb{C}[H]}V$ に一致する。以後やはり Terwilliger の表記に従い $T:=\mathrm{End}_{\mathbb{C}[H]}V$ と書くことにする。

3 The main result

本稿では次の結果を紹介する：

---

[2] **隣接作用素**と呼ぶ場合もある。

[3] 例えば [2, Theorem 1.3] を参照されたい。

[4] より正確には $\theta_i=D(q-1)-qi$ $(0\leqslant i\leqslant D)$ となる [3, Section 9.2]。

[5] この事実の表現論を用いない証明としては [8, Proposition 3] がある。

Theorem 3.1 ([12]). *Let Y denote a (not necessarily linear) code of length D over $\mathbb{F}_q$ and let $\chi_Y := \sum_{y \in Y} \hat{y} \in V$ denote the characteristic vector of Y. Set $\delta := \min\{i \neq 0 : E_i^* \chi_Y \neq 0\}$ (minimum weight) and $\delta^* := \min\{j \neq 0 : E_j \chi_Y \neq 0\}$. Suppose $t \in \{1, 2, \ldots, D\}$ is such that for every $1 \leqslant r \leqslant t$ at least one of the following holds:*

$$|\{r \leqslant j \leqslant D - r : E_j \chi_Y \neq 0\}| \leqslant \delta - r,$$
$$|\{r \leqslant i \leqslant D - r : E_i^* \chi_Y \neq 0\}| \leqslant \delta^* - r.$$

Then the supports of the words of any fixed weight in Y form a t-design.

Delsarte は Y が線型符号のとき、条件「$E_j \chi_Y \neq 0$」と条件「$E_j^* \chi_{Y^\perp} \neq 0$」が同値であることを示した [6, Chapter 6][6]。従ってこの場合 δ^* は双対符号 $Y^\perp$ の minimum weight に他ならず、Theorem 1.1 は Theorem 3.1 より導かれることに注意されたい。また、この結果を用いて例えば extended ternary Golay code の weight 3 の coset（従って非線型）から 1-design が得られることが保証される。

4 Irreducible T-modules and the displacement decomposition

前に述べたように、本稿の主結果である Theorem 3.1 は Terwilliger [16] により導入された displacement decomposition の理論の応用として得られる。ここではこの理論の一部を Hamming スキーム $H(D, q)$ の場合に話を絞って紹介する。以降 Terwilliger 代数 T の既約加群は V の部分 T-加群のみを考察する。

既約 T-加群 W の **endpoint** 及び **diameter** をそれぞれ

$$r := \min\{i : E_i^* W \neq 0\}, \quad d := |\{i : E_i^* W \neq 0\}| - 1$$

と定めると、W は次のように二通りに分解される[7]：

$$W = E_r^* W \perp E_{r+1}^* W \perp \cdots \perp E_{r+d}^* W = E_r W \perp E_{r+1} W \perp \cdots \perp E_{r+d} W$$

一例として **primary** T**-module** $M\hat{0}$ は $r = 0$ もしくは $d = D$ を満たす唯一の既約 T-加群として特徴付けられる。この二つのパラメータに関して Caughman [5, Lemmas 5.1, 7.1] は $2r + d \geqslant D$ が成立することを示した。

Terwilliger により新たに導入された W の **displacement** とは次で定義されるパラメータである：

$$\eta := 2r + d - D$$

Caughman の不等式及び $r \leqslant D, r + d \leqslant D$ より $0 \leqslant \eta \leqslant D$ である。そこで各 $0 \leqslant \eta \leqslant D$ に対し displacement が η となる既約 T-加群全ての和を V_η とすると

$$V = V_0 \perp V_1 \perp \cdots \perp V_D$$

[6] [3, Section 2.10] も合わせてご参照下さい。

[7] 一般の P-& Q-多項式スキームについては、後者の分解では r 及び d をそれぞれ $r^* := \min\{j : E_j W \neq 0\}$ (dual endpoint), $d^* := |\{j : E_j W \neq 0\}| - 1$ (dual diameter) に置き換える。

が成立する [16, Lemma 4.4]。Terwilliger はこれを V の **displacement decomposition** と呼んだ。

次に各 $0 \leqslant i, j \leqslant D$ に対し

$$V_{ij} = \left(\sum_{k=0}^{i} E_k^* V\right) \cap \left(\sum_{\ell=0}^{j} E_\ell V\right)$$

と定めると、明らかに $V_{i-1,j}, V_{i,j-1} \subseteq V_{ij}$ となる。そこで $\tilde{V}_{ij} := V_{ij} \cap (V_{i-1,j} + V_{i,j-1})^\perp$ とおくと、Terwilliger はさらに直和分解

$$V_{k\ell} = \sum_{i=0}^{k} \sum_{j=0}^{\ell} \tilde{V}_{ij}$$

が成立することを示した [16, Theorem 5.7][8]。特にここで $k = \ell = D$ とおくと次の **split decomposition** を得る：

$$V = \sum_{i=0}^{D} \sum_{j=0}^{D} \tilde{V}_{ij}$$

これら二種類の直和分解は次のように密接に関係している。すなわち

$$V_\eta = \sum_{\substack{0 \leqslant i,j \leqslant D \\ i+j=D+\eta}} \tilde{V}_{ij} \quad (0 \leqslant \eta \leqslant D)$$

が成立する [16, Theorem 6.2]。従って split decomposition は displacement decomposition の細分となっているが、$\eta < 0$ のとき $V_\eta = 0$ であることから、$i + j < D$ となる i, j については $\tilde{V}_{ij} = V_{ij} = 0$ となることが直ちに結論される。

以後我々は V_0 に注目する。この空間の重要性は今後の研究に於いてますます明らかになっていくものと思われるが、主結果である Theorem 3.1 もまたこの空間に関する基本的な性質を用いて証明される。まず、primary T-module $M\hat{0}$ は $r = 0$ かつ $d = D$ であり、従って V_0 に含まれる。また上に述べたことから直和分解

$$V_0 = \sum_{i=0}^{D} V_{i,D-i}$$

を得る。この式から次の様な V_0 の幾何学的解釈が可能になる。新たな記号 $\circ(\notin \mathbb{F}_q)$ を準備し、集合 $\mathcal{L} := (\mathbb{F}_q \cup \{\circ\})^D$ 上に半順序「$u \preccurlyeq v \iff u_i = \circ$ or $u_i = v_i$ $(1 \leqslant i \leqslant D)$」を入れると、極めて強い正則性を持った半束構造となることが知られている [7][9]。明らかに $(\mathcal{L}, \preccurlyeq)$ は次数付き (graded) であり、ランク関数は $\mathrm{rank}(u) = |\{i : u_i \neq \circ\}|$ で与えられる。特に Hamming スキーム $\mathrm{H}(D, q)$ の頂点集合 $\mathbb{F}_q^D$ は $(\mathcal{L}, \preccurlyeq)$ の top fibre、すなわちランクが最大の対象全体であることに注意されたい。さて、$u \in \mathcal{L}$ を $u \preccurlyeq \mathbf{0}$ を満たすランク t の任意の対象とする。言葉を変えると、u は 0 もしくは $\circ$ のみを成分に持つと

[8]ただし、一般に直交直和とは限らない。

[9]Hamming (semi)lattice と呼ばれる。

する。部分集合 $C_{\succcurlyeq u} := \{x \in \mathbb{F}_q^D : u \preccurlyeq x\}$ の特性ベクトルを $\chi_{\succcurlyeq u}$ と書くと、実は $\chi_{\succcurlyeq u}$ は $V_{D-t,t}$ に含まれるのである [7][10]。しかも Hamming スキームの場合 V_0 はこれらのベクトル達で生成されることまで確かめられる。

なお $C_{\succcurlyeq u}$ がそれ自身 Hamming スキーム $\mathrm{H}(D-t,q)$ の構造を持つ線型符号になっていることは一目瞭然である。従って $v \in \mathcal{L}$ を $v \preccurlyeq 0$ を満たす別のランク t の対象とすると、$C_{\succcurlyeq u}$ と $C_{\succcurlyeq v}$ は同じ重み分布を持つ。特性ベクトルを用いると、このことは次の様に言い換えられる：

$$\chi_{\succcurlyeq u} - \chi_{\succcurlyeq v} \in V_{D-t,t} \cap (M\hat{0})^{\perp} \tag{1}$$

5 Proof of Theorem 3.1

以上の準備の下で Theorem 3.1 の証明の概略を述べる。ただしここでは証明の細部には立ち入らず、Theorem 3.1 が如何に Terwilliger 代数の言葉を用いて解釈されるか、ということに重点を置く。定理の仮定及び結論は次のようなものであった：

仮定： For every $1 \leqslant r \leqslant t$ at least one of the following holds:

$$|\{r \leqslant j \leqslant D-r : E_j\chi_Y \neq 0\}| \leqslant \delta - r$$
$$|\{r \leqslant i \leqslant D-r : E_i^*\chi_Y \neq 0\}| \leqslant \delta^* - r$$

結論： The supports of the words of any fixed weight in Y form a t-design.

まず定理の仮定を考察する。W を displacement 0 を持つ既約 T-加群とすると、前に述べたように endpoint r に関して

$$W = E_r^*W \perp E_{r+1}^*W \perp \cdots \perp E_{D-r}^*W = E_rW \perp E_{r+1}W \perp \cdots \perp E_{D-r}W$$

と分解される。ここで $1 \leqslant r \leqslant t$ と仮定すると、Terwilliger 代数の基本的な性質を用いて χ_Y が W と直交することを示すことができる。詳細は [12] をご覧いただくことにして、ここでは仮定中の添え字 i, j の範囲が正に上の分解に現れる固有空間及び subconstituent と対応していることのみ注意しておく。なお、このことは次と同値である[11]：

$$T\chi_Y|_W \subseteq \sum_{j=t+1}^{D-r} E_jW$$

左辺は T-加群であるが、$1 \leqslant r \leqslant t$ のとき右辺は既約 T-加群である W の真部分空間となることからこの主張は明らかである。一方 $r > t$ の場合右辺は W に等しいので、結局この包含関係は $r > 0$ のとき常に成り立つことが分かる。Displacement 0 かつ endpoint

[10] この部分集合は Introduction で述べた Brouwer たちによる width・dual width の理論の中心的対象の一つで、現在盛んに研究されている [4, 11, 9]。

[11] 左辺は W への直交射影を意味する。

0 の既約 T-加群は primary T-module $M\hat{0}$ のみであるから、$U_0 := V_0 \cap (M\hat{0})^{\perp}$ とおくと次を得る：

$$T\chi_Y|_{U_0} \subseteq \sum_{j=t+1}^{D} E_j U_0 \tag{2}$$

次に定理の結論を考察する。各 k に対し次は同値である：

(a) The supports of the words of weight k in Y form a t-design.

(b) The *complements* of the supports of the words of weight k in Y form a t-design.

前節で述べた Hamming スキームに付随する半束構造 $(\mathcal{L}, \preccurlyeq)$ から、ランク t かつ「0 以下」の対象 u を取る。このとき $E_k^*\chi_Y$ が Y の weight k の元全体の集合の特性ベクトルであることに注意すると、(b) はさらに次と同値であることが結論される：

(c) $\langle E_k^*\chi_Y, \chi_{\succcurlyeq u}\rangle$ depends only on k, t and is independent of the choice of u.

最後に $v \in \mathcal{L}$ を同様の条件を満たす任意の対象とすると、(1) 及び $V_{D-t,t}$ の定義より

$$\chi_{\succcurlyeq u} - \chi_{\succcurlyeq v} \in V_{D-t,t} \cap (M\hat{0})^{\perp} \subseteq \sum_{j=0}^{t} E_j U_0 \tag{3}$$

を得る。この包含関係及び (2) より $\chi_{\succcurlyeq u} - \chi_{\succcurlyeq v}$ が $T\chi_Y$ と直交していることが導かれるが、まさにこれは (c) が成立することを示している。 [証終]

本稿では符号理論に於いて極めて重要かつ古典的な結果である Assmus-Mattson の定理を Terwilliger 代数の立場から見直した。ここで用いたアプローチは Terwilliger 代数の理論が符号理論に対しても非常に有効であることの一端を示していると思われる。なお主結果である Theorem 3.1 は「線型」という仮定を落とした点で従来の Assmus-Mattson の定理より若干強力であるが、実際その証明は任意の P-& Q-多項式スキーム上の符号に対しても有効であることを強調したい。

参考文献

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, J. Combin. Theory 6 (1969) 122-151.

[2] E. Bannai and T. Ito, Algebraic combinatorics I, Benjamin/Cummings, Menlo Park, 1984.

[3] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance-regular graphs, Springer-Verlag, Berlin, 1989.

[4] A. E. Brouwer, C. D. Godsil, J. H. Koolen and W. J. Martin, Width and dual width of subsets in polynomial association schemes, J. Combin. Theory Ser. A 102 (2003) 255-271.

[5] J. S. Caughman, IV, The Terwilliger algebras of bipartite P- and Q-polynomial schemes, Discrete Math. 196 (1999) 65-95.

[6] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. Suppl. No. 10 (1973).

[7] P. Delsarte, Association schemes and t-designs in regular semilattices, J. Combinatorial Theory Ser. A 20 (1976) 230-243.

[8] D. Gijswijt, A. Schrijver and H. Tanaka, New upper bounds for nonbinary codes based on the Terwilliger algebra and semidefinite programming, J. Combin. Theory Ser. A 113 (2006) 1719-1731.

[9] R. Hosoya and H. Suzuki, Tight distance-regular graphs with respect to subsets, European J. Combin. 28 (2007) 61-74.

[10] A. Schrijver, New code upper bounds from the Terwilliger algebra and semidefinite programming, IEEE Trans. Inform. Theory 51 (2005) 2859-2866.

[11] H. Tanaka, Classification of subsets with minimal width and dual width in Grassmann, bilinear forms and dual polar graphs, J. Combin. Theory Ser. A 113 (2006) 903-910.

[12] H. Tanaka, New proofs of the Assmus-Mattson theorem based on the Terwilliger algebra, submitted; arXiv:math.CO/0612740.

[13] P. Terwilliger, The subconstituent algebra of an association scheme I, J. Algebraic Combin. 1 (1992) 363-388.

[14] P. Terwilliger, The subconstituent algebra of an association scheme II, J. Algebraic Combin. 2 (1993) 73-103.

[15] P. Terwilliger, The subconstituent algebra of an association scheme III, J. Algebraic Combin. 2 (1993) 177-210.

[16] P. Terwilliger, The displacement and split decompositions for a Q-polynomial distance-regular graph, Graphs Combin. 21 (2005) 263-276; arXiv:math.CO/0306142.

[17] M. J. Todd, Semidefinite optimization, Acta Numer. 10 (2001) 515-560.