第15回代数的組合せ論シンポジウム報告集

1998年6月22日～25日

於　金沢大学工学部　秀峯会館大会議室

平成10年度文部省科学研究費基盤研究(A)

(課題番号 08304003　代表 八牧 宏美)

まえがき

この報告集は、１９９８年6月２２日(月)から２５日(木)にわたって金沢大学工学部秀峯会館で行われた「第１５回代数的組合せ論シンポジウム」の講演記録です。１００名を超える参加者を得て盛会でした。

はじめは会場を角間のニューキャンパスにある理学部に予定しておりましたが、学期中で適当な教室を予約できなかったこと、バスの便が十分でないことから、小立野の工学部秀峯会館を借りることになりました。少なからぬ混乱を生じ、ご参加の方々に迷惑をおかけいたしましたことをお詫びいたします。

この研究集会の講演者の旅費、およびこの報告集の作成に対し、科学研究費基盤研究(A)（研究代表者 熊本大学理学部教授 八牧宏美）から大きな援助をいただきました。プログラム作成にあたっては、榎本彦衛(慶應義塾大学)、坂内英一(九州大学)、吉田知行(北海道大学)、森田純(筑波大学）の４氏にお世話になりました。この場を借りて御礼申し上げます。講演者の方々、会場の準備を手伝って下さった大学院生の方々のご協力に心より感謝いたします。

１９９８年１２月

伊藤 達郎

代 数 的 組 合 せ 論

6月22日(月) - 6月25日(木)　1998
金沢大学 工学部 秀峯会館 大会議室

6月22日（月）

9.30 - 10.30　横本彦衛 (愛大 理工)
グラフの分割問題

10.40 - 11.00　小谷佳子 (東京理大 理)
Factors and Subgraphs

11.10 - 11.30　澤木俊輔 (東京理大 理)
On Rotation-, Jump-, K3-Distance Graphs

11.40 - 12.00　荻田真理子 (愛大 理工)
Difference sets in dihedral groups

13.30 - 14.00　吉田知行 (北大 理)
Species の理論入門

14.10 - 14.40　川越謙一 (金沢大 理)
3次元空間内の trivalent graph の不変量について

15.00 - 15.20　金 應烈 (神戸大 自然)　田澤新成 (近畿大 理工)　白倉暉弘 (神戸大 発達科)
1つの切断点をもつ非標識グラフの数え上げ

15.30 - 15.50　菱田隆彰 (岐阜大 工)
Possible patterns of cyclic resolutions of the BIB design
associated with PG(7,2)

16.00 - 16.20　三嶋美和子 (岐阜大 工)
Balanced bipartite block design の構成法について

16.30 - 16.50　潮 和彦 (近畿大 理工)
$\bar{S}_k$ - factorization of symmetric complete tripartite digraphs

17.00 - 17.30　山崎洋平 (阪大 理)
effective invariants of edge colourings

6月23日（火）

9.30 - 10.20　小池正夫（九大 数理）
On the theory of modular forms with respect to non-compact triangle arithmetic Fuchsian groups

10.30 - 11.10　Patrick Solé (Univ. Sophia-Antipolis)
Colored designs in q-ary codes

11.20 - 12.00　Christine Bachoc (Univ. Bordeaux)
On harmonic weight enumerators for binary codes

13.30 - 15.00　三浦晉示（ソニー, 東大生産技術研）
符号理論の最近の話題

15.20 - 15.40　斉藤直道（上智大 理工）
Laguerre Character sums

15.45 - 16.05　渡辺眞木子（九大 数理）
Possibility of dividing strongly regular graphs into two hyperplanes

16.10 - 17.30　Short Communications, Discussions, Problem Sessions

6月24日（水）

9.30 - 10.30　吉荒 聡（大阪教育大）
Higher dimensional dual hyperovals

10.45 - 11.45　鋤崎英記（阪大 理）
特殊線型群におけるデイド予想

13.30 - 14.20　和久井 道久（阪大 理）
二面体群の普遍R行列と結び目の不変量

14.30 - 14.55　竹ヶ原 裕元（室蘭工大 工）
対称群における 1 の p 乗根の個数について

14.55 - 15.20　平峰 豊（熊本大 教育）
On Sylow subgroups of abelian affine difference sets

15.30 - 15.55　奥山 京（鳥羽商船高専）
アーベル群における ADE 群について

15.55 - 16.20　城本啓介（熊本大 理）
The Singleton bounds for codes over Z_4

16.30 - 17.00　北詰正顕（千葉大 理）
Complex Leech lattice and Suzuki group

６月２５日（木）

9.00 - 9.50　堂寺知成 (放送大学 大宮学習センター)
準結晶入門

10.00 - 10.50　秋山茂樹 (新潟大 理)
Pisot 数と フラクタルタイリング

11.00 - 11.50　内藤 聡 (筑波大 数学)
有限 root 系の theta 級数に関連した組合せ論的等式について
(affine Lie 環の表現を背景として)

12.00 - 12.20　大野泰生 (阪大 理)
多重ゼータ値の関係式について

12.25 - 12.45　対島浩司 (筑波大 数学)
符号と Siegel modular form について

12.50. - 13.10　山口 学 (東大 数理)
対称群のねじれ群環と Lie superalgebra $q(n)$ の duality

プログラム責任者：22 日 榎本彦衛（慶大 理工）　23 日 坂内英一（九大 数理）
24 日 吉田知行（北大 理）　25 日 森田 純（筑波大 数学）
世話人：伊藤達郎（金沢大 理）　email: ito@kappa.s.kanazawa-u.ac.jp
電話: 076-264-6070　Fax: 076-264-6065

目次

Graph Partition Problems into Cycles and Paths

Hikoe Enomoto
Department of Mathematics
Keio University
Yokohama, 223-8522,
Japan

In this paper, we consider graph partition problems, that is, we examine sufficient conditions for the existence of vertex-disjoint subgraphs $H_1, \cdots, H_k$ such that $V(G) = \bigcup_{i=1}^{k} V(H_i)$ and each H_i satisfies some properties. We only deal with the case that the number of the subgraphs k is preassigned, and H_i is a cycle or a path. We also discuss related packing problems.

All graphs considered in this paper are finite, undirected, and without loops and multiple edges. In the following, n always denotes the order of G,

$$N_G(x) = \{y \in V(G) | xy \in E(G)\}$$

is the neighbourhood of x in G, $d_G(x) = |N_G(x)|$ is the degree of x in G,

$$\delta(G) = \min\{d_G(x) | x \in V(G)\}$$

is the minimum degree of G, and

$$\sigma_2(G) = \min\{d_G(x) + d_G(y) | xy \in E(\overline{G})\}$$

is the minimum degree sum of nonadjacent vertices. With a slight abuse of notation, for a subgraph H of G and a vertex $x \in V(G) - V(H)$, we also denote $N_H(x) = N_G(x) \cap V(H)$ and $d_H(x) = |N_H(x)|$. For a subgraph H and a subset S of $V(G)$, $d_H(S) = \sum_{x \in S} d_H(x)$. For a subset S of $V(G)$, the subgraph induced by S is denoted by $< S >$. For a subgraph H of G, $G - H =< V(G) - V(H) >$, and for a vertex x of $V(G)$, $G - x =< V(G) - \{x\} >$. For a graph G, $|G| = |V(G)|$ is the order of G, mG is the union of m copies of G, and for graphs G_1 and G_2, $G_1 \cup G_2$ is the union of G_1 and G_2, $G_1 + G_2$ is the join of G_1 and G_2. Moreover, for graphs G_1, G_2 and G_3,

$G_1 + G_2 + G_3 = (G_1 \cup G_3) + G_2$. K_n is the complete graph of order n, and K_{m_1,m_2} is the complete bipartite graph with partite sets of order m_1 and m_2. We only deal with partitions of vertices, so, "disjoint" means "vertex-disjoint."

Suppose $H_1, \cdots, H_k$ are vertex-disjoint subgraphs of G such that $V(G) = \bigcup_{i=1}^{k} V(H_i)$ and H_i is a cycle for all i, $1 \leq i \leq k$. Then the union of these H_i is a 2-factor of G with k components. A sufficient condition for the existence of a 2-factor with a specified number of components was given by Brandt et al.

Theorem 1 ([?, Theorem 3]) *Suppose $n \geq 4k$ and $\sigma_2(G) \geq n$. Then G can be partitioned into k cycles, that is, G contains k disjoint cycles $H_1, \cdots, H_k$ satisfying $V(G) = \bigcup_{i=1}^{k} V(H_i)$.*

The proof heavily depends on the following result.

Theorem 2 (Justesen [?]) *Suppose $n \geq 3k$ and $\sigma_2(G) \geq 4k$. Then G contains k disjoint cycles.*

It is quite common that if a theorem assumes that $\delta(G) \geq d$, then it still remains true if we replace the assumption with $\sigma_2(G) \geq 2d$. Theorem ?? comes from the following result of Corrádi and Hajnal by replacing δ with σ_2.

Theorem 3 ([?]) *Suppose $n \geq 3k$ and $\delta(G) \geq 2k$. Then G contains k disjoint cycles.*

Unfortunately, no proof of Theorem ?? was given in [?], and several arguments in [?] do not work under the assumption on $\sigma_2(G)$. I tried to prove Theorem ?? by myself, and found a short proof of the following slightly stronger result.

Theorem 4 ([?]) *Suppose $n \geq 3k$ and $\sigma_2(G) \geq 4k - 1$. Then G contains k disjoint cycles.*

Since the assumption $n \geq 4k$ in Theorem ?? is used only to apply Theorem ??, we can improve Theorem ?? slightly by using Theorem ??.

Theorem 1' *Suppose $n \geq 3k$ and $\sigma_2(G) \geq \max\{4k-1, n\}$. Then G can be partitioned into k cycles.*

Here, $K_{2k-1} + mK_1$ shows that the assumption $\sigma_2(G) \geq 4k - 1$ is sharp, and $K_{m,m+1}$ shows that the assumption $\sigma_2(G) \geq n$ is sharp.

Wang [?] considered partitions into cycles passing through specified edges. The following result was conjectured in [?], and was recently proved by Ishigami and Wang [?].

Theorem 5 *Suppose $k \geq 2$, $n \geq 4k-1$, and $\sigma_2(G) \geq n+2k-2$. Then for any independent edges $e_1, \cdots, e_k$, G can be partitioned into cycles $H_1, \cdots, H_k$ such that $e_i \in E(H_i)$.*

Let $e_i = x_i y_i$ and $T = \{x_1, y_1, \cdots, x_k, y_k\}$. They give the following example to show that the assumption $\sigma_2(G) \geq n+2k-2$ is sharp: Let $G = A + B + C$, where $V(A) = \{x_1\}$, $V(B) = \{x_2, \cdots, x_k, y_1, \cdots, y_k\}$, $B \cong K_{2k-1}$, and $C \cong K_m$. Then $\sigma_2(G) = n+2k-3$, while there is no cycle passing through e_1 disjoint from $T - \{x_1, y_1\}$.

Is it possible to weaken the assumption if we assume that for each i, there exists a cycle C_i with $e_i \in E(C_i)$ and $V(C_i) \cap T = \{x_i, y_i\}$? The answer is NO. Let $G = A + B + C$, where $A \cong K_k$, $B \cong K_{2k-1}$, $C \cong K_m$, $V(A) = \{x_1, \cdots, x_k\}$, and $\{y_1, \cdots, y_k\} \subset V(B)$. Then for any i, there are $k-1$ disjoint cycles $C_1, \cdots, C_{i-1}, C_{i+1}, \cdots, C_k$ satisfying $e_j \in E(C_j)$ and $V(C_j) \cap T = \{x_j, y_j\}$ for all $j \neq i$.

Is it possible to weaken the assumption if we assume the existence of k disjoint cycles $C_1, \cdots, C_k$ satisfying $e_j \in E(C_j)$ and $V(C_j) \cap T = \{x_j, y_j\}$ for $1 \leq j \leq k$? The answer is YES.

Theorem 6 (Egawa [?]) *Suppose $\sigma_2(G) \geq n+k$, $C_1, \cdots, C_k$ are disjoint subgraphs, $e_i \in E(C_i)$, and C_i is a cycle or K_2. Then there exist disjoint subgraphs $H_1, \cdots, H_k$ satisfying $V(G) = \bigcup_{i=1}^k V(H_i)$, $e_i \in E(H_i)$, and H_i is a cycle if C_i is a cycle and H_i is a cycle or K_2 if C_i is K_2.*

The sharpness of the assumption $\sigma_2(G) \geq n+k$ is shown by $K_{2k+m} + (k+m+1)K_1$ taking k edges in K_{2k+m}. The following immeditate corollary shows that we can weaken the assumption of Theorem ?? if we regard K_2 as a kind of a cycle.

Corollary 7 *Suppose $\sigma_2(G) \geq n+k$. Then for any independent edges $e_1, \cdots, e_k$, G contains disjoint subgraphs $H_1, \cdots, H_k$ satisfying $V(G) = \bigcup_{i=1}^k V(H_i)$, $e_i \in E(H_i)$, and H_i is a cycle or K_2.*

Is it possible to weaken the assumption of Theorem 1 (or Theorem 1') if we regard K_2 and K_1 as degenerated cycles?

Conjecture 1 *Suppose $\sigma_2(G) \geq n-k+1$. Then G contains k disjoint subgraphs $H_1, \cdots, H_k$ satisfying $V(G) = \bigcup_{i=1}^k V(H_i)$ and H_i is a cycle, K_2 or K_1.*

What happens if we give k distinct vertices $x_1, \cdots, x_k$ instead of independent edges and require $x_i \in V(H_i)$?

Theorem 8 *Suppose $k \geq 2$, $n \geq 3k$, and $\sigma_2(G) \geq n+2k-2$. Then for any distinct vertices $x_1, \cdots, x_k$, there exist k disjoint cycles $C_1, \cdots, C_k$ such that $x_i \in V(C_i)$.*

Sketch of Proof. Let $X = \{x_1, \cdots, x_k\}$. Considering an edge-maximal counterexample G, we may assume that there exist disjoint cycles $C_1, \cdots, C_{k-1}$ such that $\sum_{i=1}^{k-1} |C_i| \leq n-3$ and $|V(C_i) \cap X| = 1$ for $1 \leq i \leq k-1$. Let $H = < \cup_{i=1}^{k-1} V(C_i) >$ and $M = G - H$. Choose $C_1, \cdots, C_{k-1}$ such that

(1) $|H|$ as small as possible.

(2) Subject to (1), $d_M(x)$ as large as possible, where x is the unique vertex in $X - V(H)$.

We may assume that $V(C_i) \cap X = \{x_i\}$.

Claim $N_M(x_k) = V(M) - \{x_k\}$

Proof. Suppose x_k is nonadjacent with $u \in V(M) - \{x_k\}$. Then $|N_M(x_k) \cap N_M(u)| \leq 1$. (Otherwise, there is a cycle containing x_k in M.) Then $d_M(x_k) + d_M(u) \leq |M| - 1$, and $d_H(x_k) + d_H(u) \geq \sigma_2(G) - (|M| - 1) > |H| + 2(k-1)$. This implies that $d_{C_i}(x_k) + d_{C_i}(u) \geq |C_i| + 3$ for some i. Then C_i must be a triangle by (1). Let $z \in V(C_i) - \{x_i\}$. Then z is adjacent with x_k and $< (V(C_i) - \{z\}) \cup \{u\} >$ is a triangle containing x_i. This contradicts (2). ∎

Let u and v be any two neighbours of x_k in M. Then $d_M(u) + d_M(v) = 2$. Hence $d_H(u) + d_H(v) \geq n + 2k - 4 > |H| + 2(k-1)$. This implies that $d_{C_i}(u) + d_{C_i}(v) \geq |C_i| + 3$ for some i. Then C_i must be a triangle by (1). We may assume that $i = 1$, and let $V(C_1) = \{x_1, y, z\}$. If $w \in N_M(y) - \{u, v\}$, then $< \{x_k, w, u, y\} >$ and $< \{x_1, v, z\} >$ are disjoint cycles in $< V(C_1) \cup V(M) >$. Hence $N_M(y) = \{u, v\}$. Similarly, $N_M(z) = \{u, v\}$. If $k = 2$, $d_G(x_k) + d_G(y) \leq n + 1 < \sigma_2(G)$, a contradiction. So, we may assume $k \geq 3$, and then

$$\sum_{i=2}^{k-1} d_{C_i}(\{u, v, x_k, y\}) > \sum_{i=2}^{k-1} (2|C_i| + 4).$$

Hence, for some i, $d_{C_i}(\{u, v, x_k, y\}) \geq 2|C_i| + 5$. This implies that C_i is a triangle, and $d_{C_i}(\{u, v, x_k\}) \geq 8$. Then $< V(C_i) \cup \{u, v, x_k\} >$ contains two disjoint triangles such that one of them contains x_i and the other contains x_k. ∎

Theorem 9 *Suppose $k \geq 2$, $n \geq 3k$, and $\sigma_2(G) \geq n + 2k - 2$. Then for any distinct vertices $x_1, \cdots, x_k$, G can be partitioned into cycles $H_1, \cdots, H_k$ such that $x_i \in V(H_i)$.*

Proof. By Theorem ??, there exist k disjoint cycles $C_1, \cdots, C_k$ such that $x_i \in V(C_i)$. Let e_i be an edge of C_i incident with x_i. By Theorem ??, G can be partitioned into cycles $H_1, \cdots, H_k$ such that $e_i \in V(H_i)$. ∎

Let $G = K_k + K_{2k-1} + K_m$ and take k vertices in K_k. Then G does not contain such cycles, while $\sigma_2(G) = n + 2k - 3$.

If we make assumptions on the minimum degree of G, we can prove the following result:

Theorem 10 ([?]) *Suppose one of the followings holds:*
(1) $n = 3k$ *and* $\delta(G) \geq (7k-2)/3$.
(2) $3k+1 \leq n \leq 4k$ *and* $\delta(G) \geq (2n+k-3)/3$.
(3) $4k \leq n \leq 6k-2$ *and* $\delta(G) \geq 3k-1$.
(4) $n \geq 6k-2$ *and* $\delta(G) \geq n/2$.
Then for any distinct vertices $x_1, \cdots, x_k$, G *can be partitioned into cycles* $H_1, \cdots, H_k$ *such that* $x_i \in V(H_i)$.

The assumption on the minimum degree is sharp in all cases. Let $G = (A + K_{2k/3-1,2k/3+1} + K_{2k/3}) + B$, where $A \cong K_{2k/3}$, $B \cong K_{k/3}$, and $V(A) \cup V(B) = \{x_1, \cdots, x_k\}$. Then G cannot be partitioned into triangles $T_1, \cdots, T_k$ such that $|V(T_i) \cap (A \cup B)| = 1$, while $\delta(G) = (7k-3)/3$. Let $G = (A + K_{2a-1} + K_a) + B$, where $a = (n-k+1)/3$, and $A \cong K_a$ and $B \cong K_{k-a}$. Then $\delta(G) = (2n+k-4)/3$. Also, $\delta(K_k + K_{2k-1} + K_{n-3k+1}) = 3k-2$ when $n \geq 4k$ and $\delta(K_{(n-1)/2,(n+1)/2}) = (n-1)/2$.

For packing problem, it appears that the assumption in (4) is not sharp, and I conjecture the following.

Conjecture 2 *Suppose* $\delta(G) \geq 3k-1$ *and* $n < \delta(G)^2 - (3k-4)\delta(G) - 2k + 3$. *Then for any distinct vertices* $x_1, \cdots, x_k$, *there exist* k *disjoint cycles* $C_1, \cdots, C_k$ *such that* $x_i \in V(C_i)$.

When can we find a partition into paths? It is easily proved that if $\sigma_2(G) \geq n-k$, then G can be partitioned into k disjoint paths. Also, if $\sigma_2(G) \geq n$, then for any k distinct vertices $x_1, \cdots, x_k$, G can be partitioned into paths H_i such that x_i is a terminal vertex of H_i. What happens if we specify both terminal vertices?

Theorem 11 ([?]) *Suppose* $k \geq 2$, $n \geq 4k-2$, *and* $\sigma_2(G) \geq n+2k-3$. *Then either*
(1) *for any* $2k$ *distinct vertices* $x_1, y_1, \cdots, x_k, y_k$, G *can be partitioned into paths* $H_1, \cdots, H_k$ *such that* H_i *connects* x_i *and* y_i,
or
(2) $k = 2$ *and* G *is a spanning subgraph of* $K_{m+4} + (m+3)K_1$.

Suppose a partition $n = \sum_{i=1}^{k} a_i$ is given and we want to find a partition of G satisfying $|H_i| = a_i$. To partition a graph into cycles of specified lengths, there is a long-standing conjecture of El-Zahar [?].

Conjecture 3 *Suppose* $n = \sum_{i=1}^{k} a_i$ *with* $a_i \geq 3$ *for* $1 \leq i \leq k$, *and* $\delta(G) \geq \sum_{i=1}^{k} \lceil a_i/2 \rceil$. *Then* G *can be partitioned into cycles of length* $a_1, \cdots, a_k$.

The case $k = 2$ was proved in [?], and the case $k \geq 3$ is still open except the case that almost all $a_i = 3$. If $a_i = 3$ for all i, we can apply Theorem ??. Wang [?] solved a more general situation.

Theorem 12 *Suppose $n \geq 3k+3$ and $\delta(G) \geq (n+k)/2$. Then G can be partitioned into disjoint cycles $C_1, \cdots, C_{k+1}$ such that $|C_i| = 3$ for $1 \leq i \leq k$.*

We can replace δ with σ_2 in Theorem ??.

Theorem 13 *Suppose $n \geq 3k+3$ and $\sigma_2(G) \geq n+k$. Then G can be partitioned into disjoint cycles $C_1, \cdots, C_{k+1}$ such that $|C_i| = 3$ for $1 \leq i \leq k$.*

Sketch of Proof. If $n = 3(k+1)$, $\sigma_2(G) \geq n+k = 4(k+1)-1$. By Theorem 4, G contains $k+1$ cycles, which give a partition of G into triangles. Hence we may assume that $n \geq 3k+4$. By Theorem 5 of [?], G contains k disjoint triangles $C_1, \cdots, C_k$. Let $H =< \cup_{i=1}^{k} V(C_i) >$, $M = G - H$, and P a longest path in M. Choose $C_1, \cdots, C_k$ such that $|P|$ is as large as possible. Suppose $V(P) \neq V(M)$, and let x be a terminal vertex of P, and $y \in V(M) - V(P)$. Then $d_M(x) + d_M(y) \leq |M| - 2$. Hence $d_H(x) + d_H(y) \geq \sigma_2(G) - (|M| - 2) = |H| + k + 2$, which implies $d_{C_i}(x) + d_{C_i}(y) \geq 5$ for some i. Then there exists a vertex $z \in N_{C_i}(x)$ such that $< (V(C_i) - \{z\}) \cup \{y\} >$ is a triangle. This contradicts the choice of the triangles. Hence P is a Hamilton path of M. Let $P = (x_1, \cdots, x_m)$. By the same arguments as above, $d_{C_i}(x_1) + d_{C_i}(x_m) \geq 5$ for some i. We may assume that $i = k$, $V(C_k) = \{x_0, y, y'\} \subset N(x_1)$, and $\{y, y'\} \subset N(x_m)$. Let $L =< V(M) \cup V(C_k) >$. Note that x_0 and x_{m-1}, x_2 and y, and x_2 and y' are nonadjacent. (Otherwise, $< V(M) \cup V(C_k) >$ can be partitioned into a triangle and a cycle.) Let $P_0 = (x_0, x_1, \cdots, x_{m-1})$ and $P_2 = (x_2, \cdots, x_m, y)$. Then $d_{P_0}(x_0) + d_{P_0}(x_{m-1}) \leq m-1$, $d_P(x_1) + d_P(x_m) \leq m-1$, and $d_{P_2}(x_2) + d_{P_2}(y) \leq m-1$. It is not difficult to show that if there are 13 edges or more between $\{x_0, x_1, x_2, x_{m-1}, x_m, y\}$ and $V(C_i)$ for some i, $1 \leq i \leq k-1$, then $< V(M) \cup V(C_k) \cup V(C_i) >$ can be partitioned into two triangles and a cycle. Hence

$$d_L(\{x_0, x_1, x_2, x_{m-1}, x_m, y\}) \geq 3\sigma_2(G) - 12(k-1) \geq 3m + 12.$$

If x_0 and x_m are adjacent, then x_2 and x_0, x_{m-1} and y, and x_{m-1} and y' are nonadjacent. Hence $d_L(x_0) + d_L(x_{m-1}) \leq m+3$, $d_L(x_1) + d_L(x_m) \leq m+5$, and $d_L(x_2) + d_L(y) \leq m+3$, which is a contradiction. Hence x_0 and x_m are nonadjacent, and

$$d_L(x_0) + d_L(x_{m-1}) = d_L(x_1) + d_L(x_m) = d_L(x_2) + d_L(y) = m+4.$$

This implies that $\{x_2x_0, x_{m-1}y, x_{m-1}y'\} \subset E(G)$, and

$$d_{P_0}(x_0) + d_{P_0}(x_{m-1}) = d_P(x_1) + d_P(x_m) = d_{P_2}(x_2) + d_{P_2}(y) = m-1.$$

If y and x_{m-2} are adjacent, (y', x_{m-1}, x_m, y') and $(y, x_{m-2}, \cdots, x_1, x_0, y)$ partition L. Hence y and x_{m-2} are nonadjacent, which implies x_2 and x_{m-1} are adjacent. Similarly, x_2 and x_m are nonadjacent, and x_1 and x_3 are adjacent. Then (y', y, x_m, y') and $(x_1, x_3, \cdots, x_{m-1}, x_2, x_0, x_1)$ partition L. ∎

The problem of packing disjoint triangles was solved by Dirac [?].

Theorem 14 *Suppose $n \geq 3k$ and $\delta(G) \geq (n+k)/2$. Then G contains k disjoint triangles.*

Note that Theorem ?? is stronger than Theorem ??. (If $n = 3k$ or $n \geq 3k+3$, we can apply Theorem ?? directly. If $n = 3k+1$, we can apply Theorem ?? to $G - v$ for any $v \in V(G)$. If $n = 3k+2$, we can apply Theorem ?? to $G + K_1$.)

Theorem ?? was generalized in a different way in [?].

Theorem 15 ([?, Theorem 8]) *Suppose $s \leq k$, $n \geq 3s+4(k-s)$ and $\sigma_2(G) \geq n+s$. Then G contains k disjoint cycles $C_1, \cdots, C_k$ satisfying $|C_i| = 3$ for $1 \leq i \leq s$ and $|C_i| \leq 4$ for $s < i \leq k$.*

By combining Theorem ?? and Theorem ??, we get the following conjecture.

Conjecture 4 *Suppose $s \leq k$, $n \geq 3s+4(k-s)+3$ and $\sigma_2(G) \geq n+s$. Then G can be partitioned into $k+1$ disjoint cycles $H_1, \cdots, H_{k+1}$ satisfying $|H_i| = 3$ for $1 \leq i \leq s$ and $|H_i| \leq 4$ for $s < i \leq k$.*

Contrary to El-Zahar conjectue, it is fairy easy to prove the following:

Theorem 16 (Johansson[?]) *Suppose G is connected, $n = \sum_{i=1}^{k} a_i$, and $\delta(G) \geq \sum_{i=1}^{k} \lfloor a_i/2 \rfloor$. Then G can be partitioned into paths of order $a_1, \cdots, a_k$.*

Egawa and Ota [?] solved a more general packing problem.

Theorem 17 *Suppose G is connected, $n \geq \sum_{i=1}^{k} a_i$ and $\sigma_2(G) \geq 2\sum_{i=1}^{k} \lfloor a_i/2 \rfloor$. Then G contains disjoint paths of order $a_1, \cdots, a_k$ unless*
(1) *all $a_i = 3$ and $G = K_{k-1} + mK_2$,*
(2) *all $a_i = 3$, $k \equiv 2 \bmod 3$ and $G = K_1 + 3K_k$,*
or
(3) *$k = 2$, $a_1 = a_2 =$ odd, and $G = K_1 + mK_{a_1-1}$.*

When terminal vertices are specified, we conjecture the following:

Conjecture 5 *Suppose* $n = \sum_{i=1}^{k} a_i$ *and* $\sigma_2(G) \geq n + k - 1$. *Then for any* k *distinct vertices* $x_1, \cdots, x_k$, G *can be partitioned into paths* $H_1, \cdots, H_k$ *such that* $|H_i| = a_i$ *and* x_i *is a terminal vertex of* H_i.

If $a_i \neq 2$ for all i, $1 \leq i \leq k$, the assumption $\sigma_2(G) \geq n + k - 1$ cannot be weakened. (Consider $K_1 + K_k + K_m$, where $K_k = \{x_1, \cdots, x_k\}$.) This conjecture is true when $k \leq 3$ or $a_i \leq 5$ for all i [?].

With a stronger assumption, Kawarabayashi [?] proved the following.

Theorem 18 *Suppose* $n = \sum_{i=1}^{k} a_i$ *and* $\sigma_2(G) \geq \sum_{i=1}^{k} \max\{\lfloor 4a_i/3 \rfloor, a_i + 1\} - 1$. *Then for any* k *distinct vertices* $x_1, \cdots, x_k$, G *can be partitioned into paths* $H_1, \cdots, H_k$ *such that* $|H_i| = a_i$ *and* x_i *is a terminal vertex of* H_i.

More generally, we conjecture the following for packing.

Conjecture 6 *Suppose* G *is* $(k+1)$*-connected,* $n \geq \sum_{i=1}^{k} a_i$, *and* $\sigma_2(G) \geq \sum_{i=1}^{k}(a_i + 1) - 1$. *Then for any* k *distinct vertices* $x_1, \cdots, x_k$, G *contains* k *disjoint paths* $P_1, \cdots, P_k$ *such that* $|P_i| = a_i$ *and* x_i *is a terminal vertex of* P_i.

This conjecture is true when $k \leq 2$. In fact, suppose $k = 1$. Then G contains a cycle C of length $\geq \min\{n, \sigma_2(G)\} \geq a_1$ passing through x_1 [?, Theorem 2]. Deleting an edge of C incident with x_1, we get a desired path. Next, suppose $k = 2$. By [?, Corollary 1], G contains a path P connecting x_1 and x_2 with $|P| \geq \min\{n, \sigma_2(G) - 1\} \geq a_1 + a_2$. By subdividing P, we get desired paths.

Acknowledgement. The author would like to thank Y.Egawa, Y.Ishigami, H.Li, K.Ota and I.Schiermeyer for valuable discussions.

References

[1] S.Brandt, G.Chen, R.Faudree, R.J.Gould and L.Lesniak, Degree conditions for 2-factors, J. Graph Theory 24 (1997) 165-173.

[2] Corrádi and Hajnal, On the maximal number of independent circuits in graph, Acta Math. Acad. Sci. Hungar. 14 (1963) 23-439.

[3] G.A.Dirac, On the maximal number of independent triangles in graphs, Abh. Math. Semin. Univ. Hamb. 26 (1963) 78-82.

[4] Y.Egawa, private communications.

[5] Y.Egawa and K.Ota, private communications.

[6] Y.Egawa, H.Enomoto and I.Schiermeyer, in preparation.

[7] M.H.El-Zahar, On circuits in graphs, Discrete Mathematics 50 (1984) 227-230.

[8] H.Enomoto, Long paths and large cycles in finite graphs, J. Graph Theory 8 (1984) 287-301.

[9] H.Enomoto, On the existence of disjoint cycles in a graph, to appear in Combinatorica.

[10] H.Enomoto, in preparation.

[11] H.Enomoto and K.Ota, Partitions of a graph into paths with prescribed endvertices and lengths, preprint.

[12] K.Kawarabayashi, private communications.

[13] Y.Ishigami and H.Wang, private communications.

[14] R.Johansson, An El-Zahár type condition ensuring path-factors, J. Graph Theory 28 (1998) 39-42.

[15] P.Justesen, On independent circuits in finite graphs and a conjecture of Erdős and Pósa, Annals of Discrete Math. 41 (1989) 299-306.

[16] H.Wang, Covering a graph with cycles, J. Graph Theory 20 (1995) 203-211.

[17] H.Wang, Covering a graph with cycles passing through given edges, J. Graph Theory 26 (1997) 105-109.

Factors and Connected Induced Subgraphs

Keiko KOTANI
Department of Applied Mathematics
Science University of Tokyo
Shinjuku-ku,Tokyo,162-8601 Japan
e-mail:j1195701@ed.kagu.sut.ac.jp

Abstract

Let G be a connected graph without loops and without multiple edges, and let p be an integer such that $0 < p < |V(G)|$. Let f be an integer-valued function on $V(G)$ such that $2 \leq f(x) \leq \deg_G(x)$ for all $x \in V(G)$. We show that if every connected induced subgraph of order p of G has an f-factor, then G has an f- factor, unless $\sum_{x \in V(G)} f(x)$ is odd.

1 Introduction

In this paper, we consider only finite undirected graphs. Let G be a graph. We denote by $V(G)$ and $E(G)$ the set of vertices and the set of edges of G, respectively. The order of G is denoted by $|G|$. For disjoint subsets A and B of $V(G)$, we let $E(A, B)$ denote the set of edges joining A and B, and let $e(A, B)$ denote the cardinality of $E(A, B)$. A vertex x is often identified with $\{x\}$; for example, when $x \notin B$, we write $E(x, B)$ for $E(\{x\}, B)$. Also a subgraph H of G is often identified with $V(H)$; in particular, we write $G - H$ for $G - V(H)$. For $x \in V(G)$, we denote by $\deg_G(x)$ and by $N_G(x)$ the degree of x in G and the set of the vertices adjacent to x in G; thus if G has no loops and no multiple edges, $\deg_G(x) = |N_G(x)|$.

Let g, f be integer-valued functions defined on $V(G)$ such that $g(x) \leq f(x)$ for all $x \in V(G)$. A spanning subgraph F of G such that $g(x) \leq \deg_F(x) \leq f(x)$ for all $x \in V(G)$ is called a (g, f) - factor of G. If $g(x) = f(x)$ for all $x \in V(G)$, a (g, f)-factor is called an f-factor. Let $k \geq 1$ be an integer. If $f(x) = k$ for all $x \in V(G)$, an f-factor is called a k-factor. Throughout the rest of this paper, when we say that G is a multigraph, we allow G to have loops and multiple edges, and when we say that G is a graph, we assume that G has no loops and no multiple edges.

Egawa et al. [1] proved the following theorems:

Theorem A *Let G be a multigraph, and p be an integer such that $0 < p < |G|$. Let g, f be integer-valued functions defined on $V(G)$ such that $0 \leq g(x) \leq f(x) \leq \deg_G(x)$ for all $x \in V(G)$. Suppose that every induced submultigraph of order p of G has a (g,f)-factor. Then G has a (g,f)-factor unless $g(x) = f(x)$ for all $x \in V(G)$ and $\sum_{x \in V(G)} f(x)$ is odd.*

Theorem B *Let G be a connected multigraph with no loops, and let k and p be positive integers such that $0 < p < |G|$ and $k|G|$ is even. Suppose that $G - H$ has a k-factor for each connected induced subgraph H of order p. Then G has a k-factor.*

In this paper, we prove the following result related to the above theorems.

Theorem 1 *Let G be a connected graph, and p be an integer such that $0 < p < |G|$. Let f be an integer-valued function on $V(G)$ such that $2 \leq f(x) \leq deg_G(x)$ for all $x \in V(G)$. Suppose that every connected induced subgraph H of order p of G has an f-factor. Then G has an f-factor unless $\sum_{x \in V(G)} f(x)$ is odd.*

We prove several preliminary results in Section 2. In Section 3, we prove Theorem 1 and make some remarks concerning assumptions in Theorem 1.

2 Graphs with No f -Factor

The following criterion for the existence of an f-factor is essential for our proof:

Theorem C (Tutte [2]) *Let G be a graph, and let f be an integer-valued function on $V(G)$ such that $0 \leq f(x) \leq deg_G(x)$ for all $x \in V(G)$. Then G has an f-factor if and only if*

$$\delta_G(S,T) := \sum_{x \in S} f(x) + \sum_{y \in T} (deg_{G-S}(y) - f(y)) - h_G(S,T) \geq 0$$

for all disjoint subsets S and T of $V(G)$, where $h_G(S,T)$ denotes the number of components C of $G - S - T$ such that $e(T, V(C)) + \sum_{z \in V(C)} f(z) \equiv 1 \pmod 2$.

We also make use of the following lemma:

Lemma D (Tutte [2]) *Under the notation of Theorem C,*

$$\delta_G(S,T) \equiv \sum_{x \in V(G)} f(x) \pmod 2$$

for all disjoint subsets S and T of $V(G)$.

Throughout the rest of this section, we let G be a connected graph, and let f be an integer-valued function on $V(G)$ such that $2 \leq f(x) \leq \deg_G(x)$ for all $x \in V(G)$, $\sum_{x \in V(G)} f(x)$ is even, and G has no f-factor. By Theorem C, there exist disjoint subsets S and T of $V(G)$ such that $\delta_G(S,T) < 0$. Then by Lemma D,

$$\delta_G(S,T) \leq -2. \tag{2-1}$$

Under this notation, we prove the following lemmas:

Lemma 2 *Suppose that $S \neq \emptyset$. Then for each $v \in S$, $\delta_{G-v}(S-v,T) < \delta_G(S,T)$.*

Proof. Let $v \in S$. Then we obtain

$$\begin{aligned}
\delta_{G-v}(S-v,T) &= \sum_{x \in S-v} f(x) + \sum_{y \in T} (\deg_{(G-v)-(S-v)}(y) - f(y)) - h_{G-v}(S-v,T) \\
&= \sum_{x \in S} f(x) - f(v) + \sum_{y \in T} (\deg_{G-S}(y) - f(y)) - h_G(S,T) \\
&= \delta_G(S,T) - f(v) \\
&< \delta_G(S,T).
\end{aligned}$$

Hence $\delta_{G-v}(S-v,T) < \delta_G(S,T)$, as desired. ∎

Lemma 3 *Suppose that we have chosen T so that T is minimal. Suppose further that $T \neq \emptyset$. Then for each $v \in T$, $f(v) \geq deg_T(v) + 2$.*

Proof. Let $v \in T$, and set $T' = T - v$. Then we obtain

$$\begin{aligned}
\delta_G(S,T') &= \sum_{x \in S} f(x) + \sum_{y \in T'} (\deg_{(G-S)}(y) - f(y)) - h_G(S,T') \\
&\leq \sum_{x \in S} f(x) + \sum_{y \in T} (\deg_{G-S}(y) - f(y)) - \deg_{G-S}(v) + f(v) - h_G(S,T) \\
&\quad + e(v, G-S-T) \\
&= \delta_G(S,T) - \deg_T(v) + f(v).
\end{aligned}$$

Since we have $\delta_G(S,T') \geq 0$ by the minimality of T, this together with (2–1) implies $f(v) \geq \deg_T(v) + 2$. ∎

Lemma 4 *Suppose that $V(G) - S - T \neq \emptyset$ and let C be a component of $G - S - T$. Then for each subset $R \subset V(C)$, $\delta_{G-R}(S,T) \leq \delta_G(S,T) - e(R,T) + 1$.*

Proof. Let C be a component of $G - S - T$, and let $R \subset V(C)$. Then we obtain

$$\begin{aligned}
\delta_{G-R}(S,T) &= \sum_{x \in S} f(x) + \sum_{y \in T} (\deg_{(G-R)-S}(y) - f(y)) - h_{G-R}(S,T) \\
&\leq \sum_{x \in S} f(x) + \sum_{y \in T} (\deg_{G-S}(y) - f(y)) - e(R,T) - h_G(S,T) + 1 \\
&= \delta_G(S,T) - e(R,T) + 1.
\end{aligned}$$

Thus $\delta_{G-R}(S,T) \leq \delta_G(S,T) - e(R,T) + 1$, as desired. ∎

3 Proof of Theorem 1

Let G, f, p be as in Theorem 1. Suppose that G has no f-factor, and let S and T be as in the paragraph preceding the statement of Lemma 2. We assume that we have chosen S and T so that T is minimal. For an induced subgraph H of G, we often use an abbreviation $\delta(H)$ to denote $\delta_H(S \cap V(H), T \cap V(H))$. Note that $\delta(H) < 0$ implies that H has no f-factor.

Let h be the maximum integer for which there exists a sequence

$$G = H_0, H_1, \ldots, H_{h-1}, H_h = H$$

of connected induced subgraphs of G with $|H_i| = |G| - i$ satisfying :

(a) H_i is a subgraph of H_{i-1} for all $1 \leq i \leq h$, and

(b) $\delta(H_i) < 0$ for all $0 \leq i \leq h-1$, and $\delta(H) \leq -2$.

(This number h is well-defined, because the sequence consisting of a single term G satisfies (a) and (b).) If $n - h \leq p$, then there exists i $(0 \leq i \leq h)$ such that $|H_i| = p$, and by the choice of H_i, H_i is connected and has no f-factor. Therefore we may assume $|H| = n - h > p$. Let X_0 be the set of cutvertices of H; i.e., $X_0 = \{v \in V(H) \mid H - v \text{ is disconnected}\}$. Let B be an endblock of H. Here by a block of H, we mean a maximum nonseparable subgraph of H (a graph is called nonseparable if it is connected and has no cutvertex), and a block B of H such that $|V(B) \cap X_0| \leq 1$ is called an endblock of H. Also set $X = V(B) \cap X_0$. Thus if $X_0 = \emptyset$, then $B = H$ and $X = \emptyset$; if $X \neq \emptyset$, then $|X| = 1$. First we show that $(V(B) - X) \cap S = \emptyset$. Suppose that $(V(B) - X) \cap S \neq \emptyset$. Let $x \in (V(B) - X) \cap S$. Then $H - x$ is connected and $\delta(H - x) < \delta(H)$ by Lemma 2, which contradicts the maximality of h. Thus $(V(B) - X) \cap S = \emptyset$.

Case 1. $|B| = 2$.

In this case, there exists a vertex $x \in V(B)$ such that $\deg_H(x) = 1$. Let F be a connected induced subgraph of order p of H such that $x \in V(F)$. Then since $f(x) \geq 2$ by the assumption of Theorem 1, F has no f-factor.

Case 2. $|B| \geq 3$.

Subcase 2-1. $(V(B) - X) \cap T \neq \emptyset$.

Let $x \in (V(B) - X) \cap T$. We first show that $e(x, H - T) \leq 1$. Suppose that $e(x, H-T) \geq 2$. Then since $|X| \leq 1$, there exists a vertex $y \in V(H) - X - T$ such that $xy \in E(H)$. Since $e(x, H - B) = 0$ by the choice of x, it follows that $y \in V(B) - X - T$. Since $(V(B) - X) \cap S = \emptyset$, this implies $y \in V(B) - X - S - T$. Consequently, $H - y$ is connected and $\delta(H - y) \leq \delta(H) - e(y, T \cap V(H)) + 1 \leq \delta(H)$ by Lemma 4, which contradicts the maximality of h. Thus $e(x, H - T) \leq 1$, and hence $\deg_H(x) \leq (f(x) - 2) + 1 < f(x)$ by Lemma 3. Consequently, if we let F be a connected induced subgraph of order p of H such that $x \in V(F)$, then F has no f-factor.

Subcase 2-2. $(V(B)-X)\cap T=\emptyset$

In this subcase, we have $X_0\neq\emptyset$. To see this, suppose that $X_0=\emptyset$. Then $B=H$ and $X=\emptyset$. But this implies, $S\cap V(H)=T\cap V(H)=\emptyset$, and hence $\delta(H)\geq -1$, which contradicts (b). Thus $X_0\neq\emptyset$, and hence $|X|=1$.

Write $X=\{x\}$. Now we divide this subcase further into two subcases.

Subcase 2-2-1. $x\in T$.

Let $y\in N_H(x)\cap V(B)(\subset V(H)-S-T)$. Then $H-y$ is connected and $\delta(H-y)\leq \delta(H)-e(y,T\cap V(H))+1=\delta(H)$ by Lemma 4, which contradicts the maximality of h.

Subcase 2-2-2. $x\notin T$.

In this case $e(B-X,T\cap V(H))=0$ and there exists a component C of $H-S-T$ such that $B-X\subset C$. First we show that for any vertex $y\in V(B)-X$, $f(y)$ is odd. By way of contradiction, suppose that there exists a vertex $y\in V(B)-X$ such that $f(y)$ is even. Since $e(y,T\cap V(H))=0$ by the assumption of this subcase, $\sum_{x\in V(C)-y}f(x)+e(C-y\,,\,T\cap V(H))\equiv\sum_{x\in V(C)}f(x)+e(C\,,\,T\cap V(H))\ (\bmod 2)$. Therefore $h_{H-y}(S\cap V(H)\,,\,T\cap V(H))\geq h_H(S\cap V(H)\,,\,T\cap V(H))$, and hence $\delta(H-y)\leq\delta(H)$. Since $H-y$ is connected, this contradicts the maximality of h. Thus for any vertex $y\in V(B)-X$, $f(y)$ is odd. Let $y_1\in V(B)-X$. Then $H-y_1$ is connected and $\delta(H-y_1)\leq\delta(H)+1\leq -1$ by Lemma 4. There exists $y_2\in V(B)-X-y_1$ such that $H-y_1-y_2$ is connected. Since $e(\{y_1,y_2\}\,,\,T\cap V(H))=0$, $\sum_{x\in V(C)-y_1-y_2}f(x)+e(C-y_1-y_2\,,\,T\cap V(H))\equiv\sum_{x\in V(C)}f(x)+e(C\,,\,T\cap V(H))\ (\bmod 2)$. Therefore $h_{H-y_1-y_2}(S\cap V(H)\,,\,T\cap V(H))\geq h_H(S\cap V(H)\,,\,T\cap V(H))$, and hence $\delta(H-y_1-y_2)\leq\delta(H)\leq -2$, which contradict the maximality of h. ∎

We now construct examples which show that in Theorem 1, the assumption that G has no multiple edges and the assumption that f dose not take the value 1 are really necessary. Let $n,r\geq 1$ be integers and q be an integer such that $1\leq q\leq n-1$. Let M be a star such that M has center y and n endvertices $z_1,z_2,\ldots,z_n$, and y is joined to each z_k by r multiple edges. Let f be the integer-valued function on $V(M)$ defined by $f(y)=r(n-q)$, and $f(z_k)=r\ (k=1,2,\ldots,n)$. We see that if H is a connected induced submultigraph of order $n-q+1$ of M, then $y\in V(H)$, and hence H is an f-factor of H. But obviously M has no f-factor. Now if we let $r\geq 2$, the multigraph G shows that if we allow G to have multiple edges then Theorem 1 is not true; if we let $r=1$, the graph G shows that if we consider a function f on $V(G)$ such that there exists a vertex x with $f(x)=1$ then a result like Theorem 1 no longer holds.

We show another example. Let n,r,q,M be as in the above paragraph, and let m be an integer with $m>r$. Let $M_1,M_2,\ldots,M_m$ be disjoints copies of M, and for each integer j, write y_j and $z_{n(j-1)+1},z_{n(j-1)+2},\ldots,z_{nj}$ for the center and the endvertices of M_j, respectively. Let c be an integer such that $mc\equiv 0\ (\bmod r)$ and $(\frac{m}{r}-1)c\geq(r-1)q$ and set $l=q+\frac{mc}{r}$. Let L be a null graph (a graph with no edge) having l vertices, and write $V(L)=\{x_1,x_2,\ldots,x_l\}$. Let G be the multigraph define by

$$V(G)=V(L)\cup\left(\cup_{j=1}^{m}V(M_j)\right)$$

$$E(G) = \left(\bigsqcup_{j=1}^{m} \{x_i y_j | 1 \leq i \leq l\} \right) \cup \left(\bigsqcup_{j=1}^{m} E(M_j) \right).$$

Let f be the integer-valued function on $V(G)$ define by $f(x_i) = r$ $(i = 1, 2, \ldots, l)$, $f(y_j) = rn + c$ $(j = 1, 2, \ldots, m)$, and $f(z_k) = r$ $(k = 1, 2, \ldots, mn)$. We show that for every connected induced submultigraph H of order $l + m + mn - q$ of G, H has an f-factor. Let H be a connected induced submultigraph of order $l + m + mn - q$ of G. Then $\{y_1, y_2, \ldots, y_m\} \subset V(H)$. Set $a = |V(L) \cap V(H)|$, and set $b_j = |V(M_j - y_j) \cap V(H)|$ for each $1 \leq j \leq m$. Then $a + \sum_{j=1}^{m} b_j = l + mn - q$. We may assume $V(L) \cap V(H) = \{x_1, x_2 \ldots, x_a\}$. We now define a spanning submultigraph F of H by

$$\begin{aligned} E(F) &= \left(E(H) \cap \left(\bigsqcup_{j=1}^{m} E(M_j) \right) \right) \\ &\cup \left(\bigsqcup_{j=1}^{m} \left\{ x_i y_j \left| \left(\sum_{h=1}^{j-1} ((n - b_h)r + c) \right) + 1 \leq i \leq \sum_{h=1}^{j} ((n - b_h)r + c) \right. \right\} \right) \end{aligned}$$

(subscripts of the letter x are to be read modulo a). Then F is an f-factor of H. But obviously G has no f-factor. Now if we let $r \geq 2$, the multigraph G shows that if we allow G to have multiple edges then Theorem 1 is not true; if we let $r = 1$, the graph G shows that if we consider a function f on $V(G)$ such that there exists a vertex x with $f(x) = 1$ then a result like Theorem 1 no longer holds.

Acknowledgment. I would like to thank Professor Yoshimi Egawa for the help he gave to me during the preparation of this paper.

References

[1] Y. Egawa, H. Enomoto and A. Saito, Factors and induced subgraphs, *Discrete Mathematics* **68** (1988), 179-189.

[2] W.T.Tutte, The factors of graphs, *Canad.J.Math.* **4** (1952), 314-328.

Difference Sets in Dihedral Groups

Mariko Hagita
Department of Mathematics
Faculty of Science and Technology, Keio University

Definition
A k-subset D of an group G of order v is called a (v, k, λ)-difference set of G if the list of "differences"

$$\{xy^{-1}(x, y \in D)\}$$

contains each nonidentity element of G exactly λ times. We call $n := k - \lambda$ the order of D.

Definition
The group

$$D_{2l} :=< a, b | a^l = b^2 = 1, bab^{-1} = a^{-1} >$$

of order $2l$ is called dihedral group.

Existence of difference sets in non-abelian groups are not so much known.

But it seems that the number of difference sets in non-abelian groups is much less than that of abelian groups.

For example,

Theorem 1
Suppose D is a non-trivial $(2^l, k, \lambda)$-difference set in a generalized quaternion group

$$Q_{2^l} :=< a, b | a^{2^{l-1}} = 1, bab^{-1} = a^{-1}, b^2 = a^{2^{l-2}} >,$$

then $l = 4$, $k = 6$, $\lambda = 2$.

Note that there exists a nontrivial $(2^l, k, \lambda)$-difference set for each l in the abelian group

$$Z_2 \times Z_2 \times \ldots \times Z_2.$$

In the group ring ZG, let

$$D := \sum_{d \in D} d, \quad G := \sum_{g \in G} g.$$

Also. for all $A = \sum_{g \in G} a_g g \in ZG$.

$$A^{(t)} := \sum_{g \in G} a_g g^t.$$

Then a k-subset D is a (v, k, λ)-difference set of G if and only if

$$DD^{(-1)} = n \cdot 1 + \lambda G$$

in ZG. where 1 is the identity element of G.

Let D_{2l} has a nontrivial difference set

$$D = D_1 + bD_2$$

with $D_i \subset K =< a > \cong Z_l$. Let
$D_i = \sum_{k \in [l]} d_{ki} a^k$. Then

$$\begin{aligned} DD^{(-1)} &= D_1 D_1^{(-1)} + D_1 D_2^{(-1)} b^{-1} \\ &+ bD_2 D_1^{(-1)} + bD_2 D_2^{(-1)} b^{-1} \\ &= n + \lambda < a > + \lambda b < a > . \end{aligned}$$

This implies

$$D_1 D_1^{(-1)} + D_2 D_2^{(-1)} = n + \lambda < a >.$$

$$D_1 D_2^{(-1)} = D_2 D_1^{(-1)} = \frac{1}{2} \lambda < a > .$$

Let $H :=< g | g^{2l} = 1 >$. and let

$$E_1 := \sum_{k \in [l]} d_{k1} g^{2k},$$

$$E_2 := \sum_{k \in [l]} d_{k2} g^{2k+1}$$

be elements of ZH. Then

$$E_1 E_1^{(-1)} + E_2 E_2^{(-1)} = n + \lambda < g^2 >.$$

$$E_1 E_2^{(-1)} = \frac{1}{2} \lambda g < g^2 > .$$

Hence

$$E := E_1 + E_2 := \sum_{k \in [2l]} e_k g^k$$

satisfies

$$EE^{(-1)} = n + \lambda < g >$$

and all the coefficients $e_k \in \{0, 1\}$.

We see that there is a difference set in Z_{2l} with the same parameters.

Let $k_1 = |D_1|$ and $k_2 = |D_2|$.

(Note that $k_1 + k_2 = k$). Then we see

$$k_1^2 + k_2^2 = n + \lambda l.$$

$$k_1 k_2 = \frac{\lambda l}{2}.$$

So we have

$$n = (k_1 - k_2)^2.$$

Let

$$m := k_1 - k_2 > 0. \quad n = m^2.$$

From the difference set's conditions

$$D_1 D_1^{(-1)} + D_2 D_2^{(-1)} = n + \lambda < a >.$$

$$D_1 D_2^{(-1)} = D_2 D_1^{(-1)} = \frac{1}{2}\lambda < a >.$$

we see that (for $i = 1, 2$)

$$\chi(D_i)\overline{\chi(D_i)} = n \text{ or } 0 \quad \text{for all } \chi \neq \chi_0 \text{ of } G.$$

Applying the Fourier Inversion Formula to the coeffisient of 1_K of $D_i D_i^{(-1)}$.

$$k_i = \frac{1}{l} \sum_{\chi \in K^*} \chi(D_i D_i^{(-1)}) = \frac{1}{l} k_i^2 + {}^{\exists} t_i m^2.$$

Hence

$$m^2 | (lk_i - k_i^2).$$

Then since $m = k_1 - k_2$,

$$m^2 | k_1(l - k_1) = (m + k_2)(l - m - k_2)$$

$$= k_2(l - k_2) + m(l - 2k_2) - m^2.$$

We see $m | (l - 2k_2)$, and

$$m^2 | (l - 2k_2)^2 + 4k_2(l - k_2) = l^2.$$

Let

$$l = \alpha m.$$

Ryser's Conjecture

If there exists a nontrivial difference set in a cyclic group. then the parameters $(n, v) = 1$.

Conjecture

There is no nontrivial differences set in dihedral groups

Now, we have

$$v = 2l = 2\alpha m, \quad \text{and} \quad n = m^2.$$

where $m = k_1 - k_2$, $k = k_1 + k_2$.

From some calculations. we obtain

$$k_1, k_2 = \frac{1}{2}(m^2 \pm m + \lambda).$$

$$\lambda = m(\alpha - m - \sqrt{\alpha^2 - 2\alpha m + 1}).$$

A prime p is called

self-conjugate mod e,

if $p^i \equiv -1 \pmod{e'}$ for some integer i, where e' is the p-free part of e.

If each prime divisor of n is self-conjugate mod e, then we say n is self-conjugate mod e.

If the order n of a (v, k, λ)-difference set D in G is self-conjugate mod $\exp(G)$, then n is a square and

$$\begin{aligned} & D \quad D^{(-1)} && = n \cdot 1 + \lambda G \\ \Leftrightarrow \quad & \chi(D) \quad \overline{\chi(D)} && = n \quad \text{for all } \chi \neq \chi_0 \text{ of } G \\ \Leftrightarrow \quad & \chi(D) && = \sqrt{n} u_\chi \quad \text{for all } \chi \neq \chi_0 \text{ of } G. \end{aligned}$$

where all u_χ are roots of unity.

Lemma 2 *(Ma)*

Let G: cyclic group, $z \in Z[G]$. Then

$$\chi(z) \equiv 0 \ mod\ p^r \ for\ ^\forall \chi \neq \chi_0 \ of\ G$$

$$\Rightarrow {}^\exists x_1, x_2 \in Z[G], \quad z = p^r x_1 + x_2 P$$

where P is the subgroup of G of order p.

For D_{2l}, this lemma means,

$$p|n \Rightarrow p \text{ is not self-conjugate mod } 2l.$$

Theorem 3 *(Enomoto.Hagita.Matsumoto) Let $D \subset G$: difference set with $n = m^2$,*

$$^{\exists}H \lhd G, \quad K = G/H = Z_{p^a} \times Z_w,$$

where w: odd. $(n, w) = 1$. n: self-conjugate mod $|K|$. Then

$$|H| \geq m \text{ and } \lambda \geq \frac{m(m-1)}{|H|-1}.$$

For D_{2l}, this theorem means

$$^{\exists}e|2l, (e, n) = p^a, n\text{: self-conjugate mod } e$$

$$\Rightarrow e \leq \frac{2l}{m} = 2\alpha.$$

We want to say "there is no nontivial difference set in D_{2l}", even for the parameters which have not satisfies the self-conjugate conditions.

Leung,Ma,Wong(1992) prove that if there is a nontrivial difference set in D_{2l}, then

$$\frac{\phi(n)}{n} \leq \frac{1}{2}.$$

This means, n has at least 3 distinct prime divisers.

References

[1] H.Enomoto, M.Hagita and M.Matsumoto, A note on difference sets, *J.Combin.Theory ser.A*, to appear.

[2] C.T.Fan, M.K.Siu and S.L.Ma, Difference sets in dihedral groups and interlocking difference sets, *Ars.Combin.* 20A(1985), 99-107.

[3] K.H.Leung, S.L.Ma and V.L.Wong, Difference sets in dihedral groups, *Designs, Codes and Cryptography* 1(1991), 333-338.

Introduction to species

吉田 知行 (Tomoyuki YOSHIDA)
北海道大学理学部数学科
yoshidat@math.sci.hokudai.ac.jp

1 種と母関数

現代の数え上げの組合せ論を特徴づけるものは、そこに使われている代数的な方法でしょう。実際、数え上げの組合せ論の最近の論文には、可換環論、有限群論、リー環論、対称群や線形群などの表現論、ホップ代数、それにカテゴリー論が本質的な役割を果たしています。それにともない、多くの有用な理論が生まれ、数え上げの問題に大いに役立ってきました。古くは Pólya の本や Riordan の本、最近では Aigner [Aig 79] や Wilf [Wil 94] の本に見られるように、母関数の理論というと、やや泥臭い感じがします。しかし 1960 年代からは、数え上げの組合せ論現代化の流れの中で、母関数の理論も大きな発展を遂げ、数え切れないほどの論文が書かれてきました。特に Rota による一連の論文 (1964–) [RotMu 70], [DouRS 72], [BonRSV 92] と Stanley の本 [Sta 86] の影響は大きいものがありました。全体の傾向としては、抽象化の度合いが強くなっています。

そのような流れの中で、Joyal の種 (species) の理論が登場します ([Joy 81])。種とは、各有限集合 U に、ある有限集合 $F[U]$ を対応させる規則です。全単射 $\sigma : U \longrightarrow V$ に対しては、全単射 $F[\sigma] : F[U] \longrightarrow F[V]$ が対応しています。典型的な例として、各有限集合 U に、その上の単純グラフの集合 $\mathcal{G}[U]$ を対応させることによって、グラフの種が得られます。一般に、種 F の U-成分 $F[U]$ は、有限集合 U 上の何らかの組合せ論的構造全体のなす集合と見なされます。

種 F の母関数を

$$F(t) := \sum_{n=0}^{\infty} \frac{|F[n]|}{n!} t^n \in Q[[t]] \tag{1}$$

で定義します。つまり $[n] := \{1, 2, \ldots, n\}$ 上の構造の個数 $|F[n]|$ に関する母関数というわけです。母関数よりも、母関数のもとになる種の方で仕事をしようとするのが Joyal のアイデアです。そのためには、母関数に関するいろいろな操作や演算が、種の方でもできなければなりませんが、Joyal は実際にそれが可能であることを示しました。現代の高次元カテゴリー論を念頭に置くと、Joyal の種の理論は、母関数の理論の高次元化だと思います。ここに出てきた「高次元」の意味を正確に言うのは、難しいのですが、(集合の) カテゴリーは 1 次元、ある集合は 0 次元、ある集合の元は (-1) 次元の様に次元が付いています。なにはともあれ、種の定義の正確な定義から始めることにしましょう。

定義 (Joyal 1981). 種 (species) とは、$\mathbf{Bij}_f$ から $\mathbf{Set}_f$ への関手のことです。ここで $\mathbf{Bij}_f$ は、有限集合とそれらの間の全単射のなすカテゴリーで、また $\mathbf{Set}_f$ は、有限集合とそれらの間の写像の

な十カテゴリーです。種 F による有限集合 U と射 $\sigma : U \longrightarrow V$ の像をそれぞれ、$F[U]$ および $F[\sigma] : F[U] \longrightarrow F[V]$ と書くことにします。したがって $\sigma : U \longrightarrow V$ と $\tau : V \longrightarrow W$ に対し、

$$F[\tau\circ\sigma] = F[\tau]\circ F[\sigma],\ F[1_U] = 1_{F[U]} \tag{2}$$

となっています。ふたつの種の射とは、自然変換のことです。つまり、射 $\theta : F \longrightarrow G$ は、写像の族

$$\{\theta_U : F[U] \longrightarrow G[U]\}_U$$

で、任意の全単射 $\sigma : U \longrightarrow V$ に対し、$G[\sigma]\circ\theta_U = \theta_V\circ F[\sigma]$ を満たすものです。種の母関数は (1) で定義します。

例. いくつかの用語を思い出しておきましょう。木 (tree) T とは、サイクルのない連結グラフのことです。根付き木 (rooted tree) とは、ある頂点を根として指定した木のことです。森 (forest) とは、各連結成分が木であるようなグラフのことです。根付き森 (rooted forest) とは、各連結成分が根付き木であるようなグラフのことです。(根付き) 木は空集合ではありませんが、(根付き) 森は空集合も許します。次で定義される関手 RTree, RForest. End. X は種になります。

$$\begin{aligned}
\mathsf{RTree} &: U \longmapsto (\text{rooted trees on } U):\\
\mathsf{RForest} &: U \longmapsto (\text{rooted forests on } U):\\
\mathsf{End} &: U \longmapsto \mathrm{End}(U);\\
X &: U \longmapsto \{U\}
\end{aligned}$$

これらの母関数は次で与えられます:

$$\begin{aligned}
\mathsf{RTree}(t) &= \sum_{n=1}^{\infty} \frac{u_n}{n!}\, t^n;\\
\mathsf{RForest}(t) &= \sum_{n=0}^{\infty} \frac{v_n}{n!}\, t^n;\\
\mathsf{End}(t) &= \sum_{n=0}^{\infty} \frac{n^n}{n!}\, t^n;\\
X(t) &= \exp(t)
\end{aligned}$$

ここで u_n と v_n は、n 点集合 $[n] = \{1, \ldots, n\}$ 上の、それぞれ根付き木と根付き森の個数で、Cayley の有名な公式により、$u_n = n^{n-1}, v_n = (n+1)^{n-1}$ であることはよく知られています。

2 種の理論の発展

Joyal [Joy 81] にしたがって、種の間のいろいろな演算を定義しましょう。当然のことながら、これらの演算は、種の母関数の間の演算とうまく適合している必要があります。

定義. F, G を種とする。

・和 $(F+G)[U] := F[U] + G[U]$ (直和集合)。

・積 $(F \cdot G)[U] := \coprod_{V \subseteq U} F[V] \times G[U - V]$。
・微分 $F'[U] := F[U \cup \{U\}]$。
・$*$-微分 $F^{\bullet}[U] := U \times F[U]$。
・合成 $(G \circ F)[U] := \sum_{\pi \in \Pi(U)} G[\pi] \times \prod_{B \in \pi} F[P]$ (ここで $\Pi(U)$ は、集合 U の分割の集合)。

こうしてできた種の母関数について、期待通り

$$(F+G)(t) = F(t) + G(t),\ (F \cdot G)(t) = F(t) \cdot G(t),$$
$$(F')(t) = \frac{dF(t)}{dt},\ (F^{\bullet})(t) = t\frac{dF(t)}{dt},\ (G(F))(t) = G(F(t))$$

となっています。

こうやって Joyal とそれに続くフランスの研究者は母関数の抽象的理論を作り上げて行きました。その集大成は、Bergeron-Labelle-Leroux の本 (1994) にまとめられています。この本の英訳 [BerLL 98] が 1998 年に出版されたのは私たちにとって非常な幸運でした。何しろ種の理論に関する論文の多くがフランス語で書かれていて、読むのが一苦労でしたから。

一般に、組合せ論的な数列から母関数を作り、母関数の関数等式からその係数の具体的表示を求めるというのは古典的な定跡です。しかし求まったからといって、一対一対応による組合せ論的証明を与えることにはなりません。つまり母関数を使った証明方法 [Wil 94] は、よく整備された標準的なテクニックがそろっているのですが、一対一対応を見出すという組み合わせ論的な証明方法は、依然職人芸の世界のままなのです。たとえば、$\{1, 2, \ldots, n\}$ 上の根付き木の個数 u_n の母関数

$$u(t) := \sum_{n=1}^{\infty} \frac{u_n}{n!} t^n$$

は、Pólya の関数等式

$$u(t) = t \exp(u(t))$$

を満たすことが容易に示されます。よく知られているように、Lagrange の反転公式を使えば、Cayley の公式

$$u_n = n^{n-1}$$

が得られます。それなら $(n-1)$-点集合から n-点集合への写像と根付き木の間の一対一対応を見出せるでしょうか。実際そのような一対一対応を具体的に作ることは可能です。しかしその証明が母関数を使った証明とどのように関係しているのでしょうか。この例のように、母関数の変形が何ステップにもわたり、しかも途中に Lagrange の反転公式のようなブラックボックスが入ると、もはや母関数による証明を見て一対一の対応を再構成するのは不可能になります。

数え上げの組合せ論におけるこの職人芸を定跡化したのが種の理論なのです。関数等式 $u(t) = t\exp(u(t))$ を種の記号で書くと、

$$\mathsf{RTree} \cong \mathcal{X} \cdot \exp(\mathsf{RTree})$$

ということになります。この同型を具体的に与えることは可能です。さらに「組合せ論的 Lagrange の公式」を使って、この方程式を RTree に関して解くことさえできるのです。結果として、Cayley の公式の組み合わせ論的が得られます。

こうして種の理論は母関数の理論に新たな革命をもたらしました。いろいろな数列の母関数を種の言葉で書き、関数の満たす方程式を種の同型として書き直すという仕事が実行され、種の微積分・テイラー展開・微分方程式・関数方程式など、楽しいアイデアが次々と生まれて行きました。

3 種の理論の不満

しかしながらカテゴリー論から見ると、種の理論には大きな不満があります。

(1) 第 1 の不満。種とは全単射のカテゴリー $\mathbf{Bij}_f$ から有限集合のカテゴリー $\mathbf{Set}_f$ への関手でした。しかしながら、カテゴリー論から見ると $\mathbf{Bij}_f$ とは何というカテゴリーでしょう。$\mathbf{Set}_f$ に比べると、がらがらのほとんど骨だけ (almost skeletally) のカテゴリーという感じがします。カテゴリーとしては、すべての次数の対称群 S_n (カテゴリーと見なす) の直和に同値であり、したがって種 F とは対称群 S_n が作用している有限集合 $F[n]$ の列であるとも言えます。種は、$[n] := \{1, 2, \ldots, n\}$ ($[0] := \emptyset$) 上の値 $F[n]$ で決まり、各 $F[n]$ には、対称群 S_n が作用していることに注意してください。

有限集合のカテゴリー $\mathbf{Set}_f$ からのファンクターを種の定義とすると直ちにまずいことが起こります。具体的な種 F に対して、写像 $\sigma : U \longrightarrow V$ から誘導される写像 $F[\sigma] : F[U] \longrightarrow F[V]$ がうまく定義されるとは限らないのです。たとえば、各集合上の木の集合の間の写像

$$\mathsf{Tree}[U] \longrightarrow \mathsf{Tree}[V]$$

をどうやって定義すれば良いのでしょうか。

(2) 第 2 の不満。種 F の U-成分 $F[U]$ の元は、U でラベル付けられた組み合わせ構造と考えられます。したがって種の理論では、組み合わせ構造 ($F[U]$ の元) とラベル付けが分離できません。たとえば、根付き木に関する Pólya の公式 $u(t) = t\exp(u(t))$ にしても、その種による表現にしても、森が木の直和に一意的に分解されることを表現しているのですが、そこにラベル付けが絡んで議論が複雑になっています。

(3) 第 3 の不満。種の演算がカテゴリー的でありません。たとえば積 $F \cdot G$ の定義

$$(F \cdot G)[U] := \coprod_{V \subseteq U} F[V] \times G[U - V]$$

に表れる $V \subseteq U$ も $U - V$ も $\mathbf{Bij}_f$ におけるものではありません。全単射のカテゴリー $\mathbf{Bij}_f$ では、部分対象 $V \subseteq U$ も補集合 $U - V$ も直和さえも、一般には定義されません。つまりカテゴリー論的に見ると、種の積の定義はナンセンスとしか思えないのです。

これらすべての不満を解消する方法があります。それは種の代わりに、ラベル付けされていない組み合わせ構造 (たとえば、木、森、グラフ、いろいろな代数系) のカテゴリーを考えることです。ラベル付けは、そのようなカテゴリーから有限集合のカテゴリーへの忘却関手に付随したものとして定義することができます。これを以下の節で述べて行きます。詳しくは、私の論文 [Yos 98a], [Yos 98b] を見てください。

4 母関数の理論の矢印化計画

これからやろうとするのは、母関数の理論のさらなる徹底したカテゴリー化です。カテゴリー論の参考書としては、[Mcl 71]、[MclMo 92] が良いと思います。まずカテゴリーの母関数を定義しましょう。$\mathcal{E}$ をカテゴリーで、以下の条件を満たすものとします。

(a) 骨格的小型性: $\mathcal{E}$ は、小さなカテゴリーに同値である。すなわち同型類全体 $\mathcal{E}/\cong$ が集合を成す。
(b) 局所有限性: $\mathcal{E}$ における各 Hom-set $\mathrm{Hom}(A,B)$ は有限集合である。実際は自己同型群が有限群であるとするだけで十分。

このようなカテゴリー $\mathcal{E}$ の母関数を、形式的和

$$\Phi_{\mathcal{E}}(t) := \sum_{X\in\mathcal{E}}{}' \frac{1}{|\mathrm{Aut}(X)|}\, t^X \tag{3}$$

として定義します。ここで和は $\mathcal{E}$ の対象の同型類の完全代表系を取ることを意味します。また t^X は $X\in\mathcal{E}$ を含む同型類に対応した不定元で、

$$X\cong Y \quad\Longrightarrow\quad t^X = t^Y$$

を満たすものとします。

またファンクター $F:\mathcal{E}\longrightarrow\mathcal{S}$ の母関数を

$$\Phi_F(t) := \sum_{X\in\mathcal{E}}{}' \frac{1}{|\mathrm{Aut}(X)|}\, t^{F(X)} \tag{4}$$

で定義します。この和は**各ファイバーの有限性**:

$$\sharp\{X\in\mathcal{E}\mid F(X)\cong N\}/\cong\ <\infty \tag{5}$$

のもとで well-defined です。実際

$$\Phi_F(t) = \sum_{N\in\mathcal{S}}{}' \frac{1}{|\mathrm{Aut}(X)|}\left(\sum_{F(X)\cong N}{}' \frac{|\mathrm{Aut}(N)|}{|\mathrm{Aut}(X)|}\right) t^N$$

と書けて、中の和は有限和です。

$\mathbf{Set}_f$ にベキを持つベキ級数は、普通のベキ級数と同一視します:

$$\sum_{n=0}^{\infty} a_n t^{[n]} = \sum_{n=0}^{\infty} a_n t^n.$$

定義. $F:\mathcal{E}\longrightarrow\mathcal{S}$ をファンクター、N を $\mathcal{E}$ の対象とします。N 上の $\mathcal{E}$-**構造**とは、対象 $X\in\mathcal{E}$ と同型 $\sigma: F(X)\xrightarrow{\cong} N$ の対 (X,σ) のことです，同型射 σ をラベル付けと言います，N 上のふたつの $\mathcal{E}$-構造 (X,σ) と (Y,τ) が同型であるとは、$\mathcal{E}$ の同型射 $f: X\xrightarrow{\cong} Y$ が存在して、$\sigma=\tau\circ F(f)$ を満たすことです。N 上の $\mathcal{E}$-構造の同型類の集合を $\mathrm{Str}(\mathcal{E}/N)/\cong$ と書くことにします，

定理. ファンクター $F:\mathcal{E}\longrightarrow S$ は忠実で、ファイバーの有限性 (5) を満たすとする。このとき

$$F(t)=\sum_{N\in S}{}'\frac{|\mathrm{Str}(\mathcal{E}/N)/\cong|}{|\mathrm{Aut}(N)|}\,t^N \tag{6}$$

である。

例. (1) **RTree** (**RForest**) を根付き木のカテゴリー (根付き森のカテゴリー) とします。射は、頂点集合から頂点集合への写像で、根を根に移し、辺は辺に写すものです。U : **RTree** $\longrightarrow$ $\mathbf{Set}_f$ (V : **RForest** $\longrightarrow$ $\mathbf{Set}_f$) を、根付き木 (根付き森) にその頂点集合を対応させるファンクターとします。このとき集合 N 上の **RTree**-構造 (**RForest**-構造) の同型類は、N を頂点集合とする根付き木 (根付き森) です。別の言い方では、N でラベル付けられた根付き木 (森) です。したがって、U と V の母関数は

$$U(t)=\sum_{n=1}^{\infty}\frac{u_n}{n!}\,t^n,\quad V(t)=\sum_{n=1}^{\infty}\frac{v_n}{n!}\,t^n$$

(ここで u_n, v_n は $[n]$ 上の根付き木と根付き森の個数) となります。
(2) $\mathbf{ASet}_f$ を、有限集合 X と自分自身への写像 $\alpha:X\longrightarrow X$ の対 (X,α) 全体のなすカテゴリーとします。ただし射 $f:(X,\alpha)\longrightarrow(Y,\beta)$ とは、写像 $f:X\longrightarrow Y$ で $f\circ\alpha=\beta\circ f$ を満たすものです。$F:\mathbf{ASet}_f\longrightarrow\mathbf{Set}_f:(X,\alpha)\longmapsto X$ を忘却関手とします。このとき、n-点集合 $[n]$ 上の $\mathbf{ASet}_f$-構造の同型類の集合 $\mathrm{Str}(\mathbf{ASet}_f/[n])/\cong$ と、対象半群 $T_n:=\mathrm{Map}([n],[n])$ とは一対一に対応しています:

$$\mathrm{Str}(\mathbf{ASet}_f/[n])/\cong\quad\longleftrightarrow\quad T_n.$$

したがって

$$F(t)=\sum_{n=0}^{\infty}\frac{n^n}{n!}\,t^n$$

となります。これは種 End の母関数と同じです。
(3) G を有限生成群、$\mathbf{Set}_f^G$ を有限 G-集合と G-写像のカテゴリーとします。そうすれば忘却ファンクター $F:\mathbf{Set}_f^G\longrightarrow\mathbf{Set}_f$ があります。このとき集合 $[n]$ 上の $\mathbf{Set}_f^G$-構造の同型類は、G から対称群 S_n への群準同型写像と一対一に対応します:

$$\mathrm{Str}(\mathbf{Set}_f^G/[n])/\cong\quad\longleftrightarrow\quad\mathrm{Hom}(G,S_n).$$

したがって

$$F(t)=\sum_{n-0}^{\infty}\frac{|\mathrm{Hom}(G,S_n)|}{n!}\,t^n$$

となります。

定義. ファンクター $F:\mathcal{E}\longrightarrow\mathbf{Set}_f$ の元 (elements) とは、$\mathcal{E}$ の対象 X と集合 $F(X)$ の元 a の対 (X,a) のことです。ふたつの元の間の射 $f:(X,a)\longrightarrow(Y,b)$ とは、$\mathcal{E}$ の射 $f:X\longrightarrow Y$ で $F(f)(a)=b$ を満たすものです。元のカテゴリーを $\mathrm{Elts}(F)$ で表します。

定理. (1) $F : \mathbf{Bij}_f \longrightarrow \mathbf{Set}_f$ を種とする。このとき

$$F^{\sim} : \mathsf{Elts}(F) \longrightarrow \mathbf{Set}_f ; (X, a) \longmapsto X$$

は忠実なファンクターで、ファイバーの有限性を満たす。
(2) 忠実な関手 $S : \mathcal{E} \longrightarrow \mathbf{Set}_f$ に対し、

$$S^{\sim} : \mathbf{Bij}_f \longrightarrow \mathbf{Set}_f ; N \longmapsto \mathsf{Str}(\mathcal{E}/N)/\cong$$

は種である。
(3) 種 F に対し、$F^{\sim\sim} \cong F$ である。
(4) 対応している種と忠実なファンクターの母関数は等しい。

$$F(t) = F^{\sim}(t),\ S(t) = S^{\sim}(t).$$

この定理により、忠実でファイバーの有限性を満たすファンクターは、種の概念の一般化と見なせることが分かります。

5 カテゴリーとファンクターの演算

種については、ベキ級数の演算に対応する演算が可能でした。ファンクターやカテゴリー自身についても、同様の演算があります。それらのいくつかを紹介しましょう。特に断らない限り、$\mathcal{E}, \mathcal{F}, \mathcal{S}$ はカテゴリー、$S : \mathcal{E} \longrightarrow \mathcal{S}$ と $T : \mathcal{F} \longrightarrow \mathcal{S}$ はファンクターとします。$\mathcal{S}$ は有限直和を持つと仮定します。

$I\mathcal{S}$ に対し、**コンマカテゴリー** $I \uparrow S$ は、(α, X) の形の対象を持つとして定義します。ここで $X \in \mathcal{E}$ で $\alpha : I \longrightarrow S(X)$ です。射 $f : (\alpha, X) \longrightarrow (\beta, Y)$ は、$\mathcal{E}$ における射 $f : X \longrightarrow Y$ で、$\alpha = \beta \circ F(f)$ を満たすとします。

・**和:** $S + T : \mathcal{E} + \mathcal{F} \longrightarrow \mathcal{S}$ ($\mathcal{E} + \mathcal{F}$ はカテゴリーの直和)

・**積:** $S \cdot T : \mathcal{E} \times \mathcal{F} \longrightarrow \mathcal{S} ; (X, Y) \longmapsto S(X) + T(Y)$

・**微分:** $S' : \mathsf{Elts}(S) \longrightarrow \mathbf{Set}_f ; (X, s) \longmapsto S(X) - \{s\}$ (ただし $S : \mathcal{E} \longrightarrow \mathbf{Set}_f = \mathcal{S}$ で、各 $S(f)$ は単射)

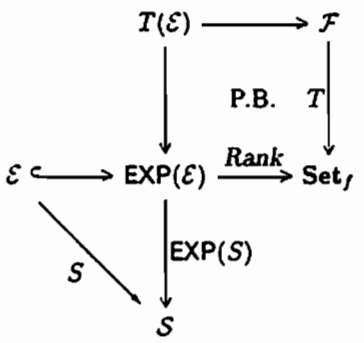
・**$*$-微分:** $S^* : \mathsf{Elts}(S) \longrightarrow \mathbf{Set}_f ; (X, s) \longmapsto S(X)$ (ただし $S : \mathcal{E} \longrightarrow \mathbf{Set}_f = \mathcal{S}$)

・**偏微分:** $\partial_I : I \uparrow \mathcal{E} \longrightarrow \mathcal{S} ; (\alpha, X) \longmapsto S(X)$

・**カテゴリーの指数関数:** カテゴリー $\mathsf{EXP}(\mathcal{E})$ を次のように定義する。対象は $(N, (Y_j)_{j \in N})$ (N は有限集合で $Y_j \in \mathcal{E}$) の形の組で、射 $(f, (\tau_i)) : (M, (X_i)) \longrightarrow (N, (Y_j))$ は、写像 $f : M \longrightarrow N$ と射の族 $\tau_i : X_i \longrightarrow Y_{f(i)}$ の組。

・**ファンクターの指数関数:** $\mathsf{EXP}(S) : \mathsf{EXP}(\mathcal{E}) \longrightarrow \mathbf{Set}_f ; (N, (Y_j)) \longmapsto \coprod_j Y_j$。

・ファンクターの合成: $T(S) : T(\mathcal{E}) \longrightarrow \mathrm{EXP}(\mathcal{E}) \longrightarrow \mathcal{S}$ を以下の様にカテゴリーの引き戻し図式で定義します。ただしここでは $S : \mathcal{E} \longrightarrow \mathcal{S}$ で、$T : \mathcal{F} \longrightarrow \mathbf{Set}_f$ としておきます。



ここで、*Rank* は、$(N, (Y_j))$ に N を対応させるファンクターです。

このようにして定義した演算は、次のように母関数の演算とうまく適合しています。

$$
\begin{aligned}
&(S+T)(t) = S(t) + T(t),\ (S \cdot T)(t) = S(t) \cdot T(t),\\
&S'(t) = \frac{dS(t)}{dt},\ S^{\bullet}(t) = t\frac{dS(t)}{dt},\\
&(\partial_I S)(t) = \sum_{X \in \mathcal{E}}{}' \frac{|\mathrm{Hom}(I, S(X))|}{|\mathrm{Aut}(X)|}\, t^{S(X)},\\
&(\mathrm{EXP}(S))(t) = \exp(S(t)),\ (T(S))(t) = T(S(t)).
\end{aligned}
$$

微分について、通常どおりの公式が成り立っています。

$$
\begin{aligned}
(S \cdot T)' &\cong S' \cdot T + S \cdot T',\\
(T(S))' &\cong S' \cdot T'(S).
\end{aligned}
$$

ここで $S : \mathcal{E} \longrightarrow \mathbf{Set}_f, T : \mathcal{F} \longrightarrow \mathbf{Set}_f$ とします。

また $I \in \mathcal{S}$ に対し、Hom ファンクター $\mathrm{Hom}(I, -)$ が $\mathcal{S}$ の有限直和を保つという条件を満たすなら、やはり同様の公式が成り立っています。

$$
\begin{aligned}
\partial_I(S \cdot T) &\cong \partial_I(S) \cdot T + S \cdot \partial_I(T),\\
S \cdot \partial_I(T(S)) &\cong T^{\bullet}(S) \cdot \partial_I(S).
\end{aligned}
$$

例. (1) $\mathbf{Surj}_f$ を有限集合の間の全射 $(X \overset{p}{\twoheadrightarrow} X')$ のなすカテゴリーとします。全射 $(X \overset{p}{\twoheadrightarrow} X')$ から全射 $(Y \overset{q}{\twoheadrightarrow} Y')$ への射は、写像 $f : X \longrightarrow X'$ と $f' : X' \longrightarrow Y'$ の対 (f, f') で $f' \circ p = q \circ f$ を満たすものです。また空集合でない有限集合のなすカテゴリーを $\mathbf{Set}_f - \{\emptyset\}$ とします。このとき

$$\mathbf{Surj}_f \cong \mathrm{EXP}(\mathbf{Set}_f - \{\emptyset\})$$

が成り立ちます。したがってファンクター

$$F : \mathbf{Surj}_f \longrightarrow \mathbf{Set}_f; (X \twoheadrightarrow X') \longmapsto X$$

の母関数を取ると、よく知られた公式

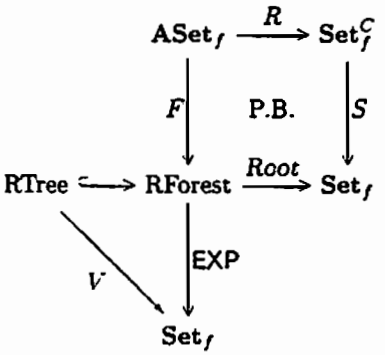
$$\sum_{n=0}^{\infty}\frac{b(n)}{n!}t^n=\exp\left(\sum_{n=1}^{\infty}\frac{t^n}{n!}\right)=\exp(e^t-1)$$

が得られます。

(2) $\mathbf{ASet}_f$ を、有限集合 X と自分自身への写像 $\alpha:X\longrightarrow X$ の対 (X,α) 全体のなすカテゴリーとします。$(X,\alpha)\in\mathbf{ASet}_f$ の根とは、ある $n\geq 1$ に対して $\alpha^n(x)=x$ となる $x\in X$ のことです。(X,α) の根の集合 $R(X,\alpha)$ には、$x\longmapsto\alpha(x)$ によって、無限巡回群 C が作用しています。これによってファンクター

$$R:\mathbf{ASet}_f\longrightarrow\mathbf{Set}_f^C:(X,\alpha)\longmapsto R(X,\alpha)$$

が得られます。次に、根付き森 $F(X,\alpha)$ を定義します。そのために、$F(X,\alpha)$ の頂点集合を X とし、$\{x,y\}$ がその辺であるということを、$\alpha(x)=y$ で x が根でないこととします。まとめると次の引き戻し図式が得られます:



ここで S は忘却ファンクターです。RForest $\cong$ EXP(RTree) に注意すると、

$$S(V):S(\mathrm{RTree})\cong\mathbf{ASet}_f\xrightarrow{F}\mathrm{RForest}\xrightarrow{V}\mathbf{Set}_f$$

が得られます。その母関数を取ると

$$(S(V))(t)=S(V(t))=\frac{1}{1-V(t)}$$

が得られます。ここで $S(t)=(1-t)^{-1}$ を使いました。さらに Cayley の公式 $V(t)=\sum_{n=1}^{\infty}n^{n-1}t^n/n!$ により、

$$\sum_{n=0}^{\infty}\frac{n^n}{n!}t^n=\frac{1}{1-\sum_{n=1}^{\infty}\frac{n^{n-1}}{n!}t^n}$$

というおもしろい公式が得られます。

6 指数関数型恒等式

指数関数型恒等式は、ラベル付けられた組み合わせ構造を数えるときによく登場します。この公式をできるだけ一般的な状況で使えるようにしようと、たくさんの研究が発表されています。指数関数型恒等式の本質は、連結な組み合わせ構造への分解の一意性にあると考えられます。しかしながら、これまでの公式の問題点は、ラベル付けというよけいなものが入り込んでいることにあります。このよけいな夾雑物を除いた指数関数型恒等式は、カテゴリーの母関数の概念を用いて表せます。

定義. $\mathcal{E}$ を例によって骨格的に小型で、局所有限なカテゴリーとします。対象 I が**連結**とは、条件

$$I \cong A + B \quad \Longrightarrow \quad A \text{ または } B \text{ が始対象}$$

を満たすことです。連結な対象全体のなす充満部分カテゴリーを $\mathrm{Con}(\mathcal{E})$ で表します。カテゴリー $\mathcal{E}$ が **KS-カテゴリー**であるとは、任意の対象 X が有限個の連結な対象の直和に同型であり、そのような直和分解 (KS-分解) が一意的なことを言います。ここで分解の一意性は次を意味します。

$$X \cong I_1 + \cdots + I_m \cong J_1 + \cdots + J_n \quad (I_\alpha, J_\beta \in \mathrm{Con}(\mathcal{E}))$$

がふたつの KS-分解のとき、$m = n$ であり、さらにある置換 $\pi \in S_n$ と射 $f_\alpha : I_\alpha \longrightarrow J_{\pi(\alpha)}$ $(\alpha = 1, \ldots, n)$ が存在して、次の図式は可換になる:

$$\begin{array}{ccc} I_\alpha & \xrightarrow{f_\alpha} & J_{\pi(\alpha)} \\ {\scriptstyle i_\alpha}\downarrow & & \downarrow{\scriptstyle j_{\pi(\alpha)}} \\ X & \xrightarrow{\mathrm{id}} & X \end{array}$$

ここで、i_α と j_β は標準的入射。

最後にカテゴリー版の**指数関数型恒等式**を紹介します。

定理. $\mathcal{E}$ が KS-カテゴリーなら、

$$\mathcal{E}(t) = \exp(\mathrm{Con}(\mathcal{E})(t))$$

である。逆にこの公式が成り立ち、標準的入射 $X \longrightarrow X + Y$ がつねに単射なら、$\mathcal{E}$ は Dress の条件を満たす KS-カテゴリーで、

$$\mathcal{E} \cong \mathsf{EXP}(\mathrm{Con}(\mathcal{E}))$$

となる。

あとは、この公式をファンクターで飛ばして、いろいろな指数関数型恒等式が得られます。プレプリント [Yos 98a] と [Yos 98b] を見てください。上の定理にでてきた Dress の条件とは、次の可換図式

$$\begin{array}{ccccc} A & \longrightarrow & C & \longleftarrow & B \\ \downarrow & & \downarrow & & \downarrow \\ X & \longrightarrow & X+Y & \longleftarrow & Y \end{array}$$

において、上の列が直和図式であるための必要十分条件がふたつの四角形が引き戻し図式であることをいいます ([Dre 73])。

7 合成の問題

$\mathcal{E}$ を有限直和を持つカテゴリーで、任意の X に対し、条件

$$\sharp\{(A,B) \mid A+B \cong X\}/\cong < \infty \tag{7}$$

を満たすものとします。このとき、可換環 R 係数でベキ指数がカテゴリー $\mathcal{E}$ の対象であるような形式的ベキ級数全体

$$R[[\mathcal{E}^{op}/\cong]] := \left\{ \sum_{X\in\mathcal{E}}{}' a_X t^X \mid a_X \in R \right\}$$

は、環になります。積はもちろん

$$t^X \cdot t^Y := t^{X+Y},\ 1 = t^0$$

を線形に拡張したものです。

このベキ級数環も普通にある演算 (和・積・微分など) を持つのですが、合成だけは一般には不可能です。たとえば $F(t) = 1+t^A$ と $G(t) = t^B$ に対し、$(G(F))(t) = (1+t^A)^B$ をどうやって定義すれば良いんでしょうか。特別な場合には合成が可能です。たとえば、ベキ級数 $f(t) = \sum_{X\in\mathcal{E}}{}' a_X t^X$ を普通の多項式 $g(t) \in Q[t]$ に代入することならできます。また全射のカテゴリー $\mathbf{Surj}_f$ の場合は Plethysm 合成があります ([Nav 87])。連結な対象は $J(n) = ([n] \xrightarrow[[1]]{} \gg)$ の形をしています ($[n] := \{1,\dots,n\}$) の形をしています。したがってベキ級数の $J(n)$ 乗を定義する必要がありますが、そのために

$$\left(\sum{}' a_{(X\to X')}\, t^{(X\to X')}\right)^{J(n)} := \sum{}' a_{(X\to X')}\, t^{(X\to X')\times J(n)}$$

とします。こうして、Plethysm 合成が定義できたことになります。

合成可能性を突き詰めていくと、どうしても多項式やベキ級数の概念を、上で定義した $R[[\mathcal{E}^{op}/\cong]]$ よりもさらに拡張する必要がでてきます。今のところカテゴリー $\mathcal{E}$ としては、局所有限トポス ([MclMo 92]) を取るのが応用のために適当と思います。さらに係数環として、丹原ファンクター (乗法的 induction を持つような Green ファンクター、たとえば有限群のコホモロジー環) T を取ります。このとき多項式環とベキ級数環を次で定義します。

$$\varinjlim T(\Omega^N), \quad \varprojlim T(\Omega^N).$$

変な定義ですが、これでも多項式環やベキ級数環の拡張になっています。これについては、私の準備中の論文 [Yos 98c] で述べる予定です。

参考文献

[Aig 79] M.Aigner, *Combinatorial Theory*, Springer, Berlin. 1979.

[BerLL 98] F.Bergeron–G.Labbelle–P.Leroux, *Combinatorial Species and Tree-like Structures*, (Encyclopedia of Mathematics and its Applications) Cambridge, 1998.

[BonRSV 92] F.Bonetti–G.-C.Rota–D.Semato–A.Venezia, On the foundation of combinatorial theory. X. A categorical setting for symmetric functions, *Studies in Appl. Math.* **86** (1992), 1–29.

[DouRS 72] P.Doubilet–G.-C.Rota–R.Stanley, On the foundations of combinatorial theory (VI): The idea of generating functions, *in* "Sixth Berkeley Symposium on Math. Stat. and Prob. vol.II: Probability Theory", 267–318, Univ. California, 1972.

[Dre 73] A.Dress, Contributions to the theory of induced representations, *in* "Representation Theory of Finite Groups and Related Topics," 182–240, LNS in Math. **342**, Springer, 1975.

[Dur 86] A.Dür, *Möbius Functions, Incidence Algebras and Power Series Representations*, LNS in Math. **1202**, Springer, Berlin, 1986.

[Joy 81] A.Joyal, Une théorie combinatoire des séries formelles, *Adv. Math.* **42** (1981), 1–82.

[Mcl 71] S.Mac Lane, *Categories for the working mathematicians*, Springer, Berlin, 1971.

[MclMo 92] S.Mac Lane–I.Moerdijk, *Sheaves in Geometry and Logic*, Springer, Berlin, 1992.

[Nav 87] O.Nava, On the combinatorics of plethysm. *J. Combin. Theory* (A) **46** (1987), 212–251.

[RotMu 70] G.-C.Rota–R.Mullin, On the Foundation of Combinatorial Theory III: theory of binomial enumeration, *in* "Graph theory and its Applications" (Haris, ed.), 167–213, Academic Press, NY., 1970.

[Sta 86] R.Stanley, *Enumerative Combinatorics* (I), Wadsworth, 1986.

[Wil 94] H.Wilf, *generatingfunctionology* (second edition) , Academic Press, NY., 1994.

[Yos 96] T.Yoshida, Classical problems in group theory (I): Enumerating subgroups and homomorphisms, *Sugaku Expositions* **9** (1996),169–184.

[Yos 98a] T.Yoshida, Categorical aspects of generating functions (I), Exponential formulas and Krull-Schmidt categories, Hokkaido Univ. Preprint Series in Math., # 416, June 1998

[Yos 98b] T.Yoshida, Categorical aspects of generating functions (II), Operations on categories and functors, Hokkaido Univ. Preprint Series in Math., # 432, June 1998

[Yos 98c] T.Yoshida, Categorical aspects of generating functions (III), The rings of polynomials and power series with exponents in a locally finite topos, (in preparation).

On Invariants of Trivalent Graphs

Kenichi Kawagoe
Computational Science
Faculity of Science
Kanazawa University
Kakuma-machi Kanazawa JAPAN
e-mail:kawagoe@kappa.s.kanazawa-u.ac.jp

Abstract

In this article, we construct invariants of graphs in $\mathbb{R}^3$, especially trivalent graphs.

1 Introduction

In this paper, we will discuss invariants of undirected graphs in S^3 [2] [3] [4], especially trivalent graphs in S^3, and we represent graphs as diagrams on S^2. For an graph diagram G on S^2, we introduce the following five transformations (I), (II), (III), (IV), (V).

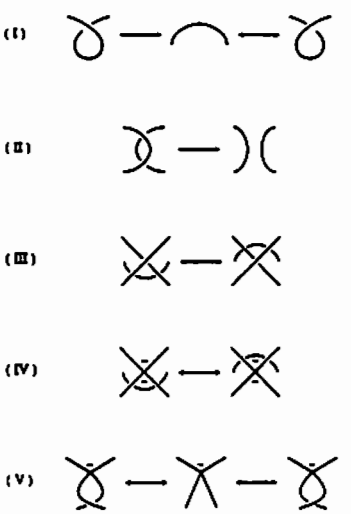


Figure 1:

If two graph diagrams are transformed to each other by finite sequences of

moves (I), ..., (V), then we call two diagram equivalent. We want to construct functions from the graph diagrams which are invariant under such moves. For our request, we make use of invariants of knots and links. They are Homfly polynomials and Kauffman polynomials. But we modify them as regular isotopy invariants which are invariant under the moves (II) and (III) and change under the move (I) by some scalar constants.

2 Skeins associated with Homfy and Kauffman polynomials

In this section, we will prepare terminologies, definitions and lemmas from knot theory.

Let a, q be complex parameters. For an integer n, $[n]$ and $[n]_a$ are defined as

$$\begin{aligned} [n] &= \frac{q^n - q^{-n}}{q - q^{-1}} \\ [n]_a &= \frac{aq^n - a^{-1}q^{-n}}{q - q^{-1}} \end{aligned}$$

and for integers $n \geq k \geq 0$ are positive, $[n]!$ and $\begin{bmatrix} n \\ k \end{bmatrix}$ are defined by

$$\begin{aligned} [n]! &= [n][n-1]\cdots[1]. \\ \begin{bmatrix} n \\ k \end{bmatrix} &= \frac{[n]!}{[k]![n-k]!} \end{aligned}$$

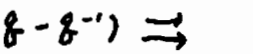
where we define $[0]! = 1$.

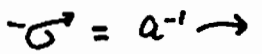
In next subsections, we discuss Homfly case and Kauffman case. To avoid using many symbols, we may use same symbols unless we are not confused. In diagrams, when there is an integer n beside an arc, it means n arcs parallel with the original one.

2.1 Homfly case

We consider diagrams of oriented links and n oriented arcs on a surface F. There are $2n$ points $p_1, \ldots, p_{2n}$ on the boundary of F, which are n outgoing points and n incoming points and the terminals of the arcs are at these $2n$ points, compatible with the orientations of the points. A complex vector space $\mathcal{S}(F) = \mathcal{S}(F, \{p_1, \ldots, p_{2n}\})$ consists of formal linear sums of such a diagrams quotiented by

(1) regular isotopy and $D \cup \bigcirc = [0]_a\, D$

(2) 

(3) 

where D is any diagram in F and $\bigcirc$ is null-homotopic in F. We call the complex vector space $\mathcal{S}(F, \{p_1, \ldots, p_{2n}\})$ a linear skein associated with Homfly polynomials It is well-known that if we take S^2 with no points as F, then $\mathcal{S}(S^2)$ is equal to $\mathbb{C}$ and if the diagram is only one link diagram with the coefficient 1, the corresponding complex value is the Homfly polynomial of the link. We consider a square with $2(n+m)$ points $n+m$ points are located on the left side and incoming n points are on the upper side and outgoing m points are on the lower side, the other $n+m$ points are located on the right side and outgoing n points are on the upper side and incoming m points are on the lower side. We denote this square with $2(n+m)$ by $H_{n,m}$. On $\mathcal{S}(H_{n,m})$, we can define a multiplication by setting two elements left and right, and then connecting straightforwardly left outgoing n (incoming m) points with right incoming n (outgoing m) points. By this multiplication, $\mathcal{S}(H_{n,m})$ become an algebra over $\mathbb{C}$. We denote the identity element by $1_{n,m}$, which is the straight $n+m$ strings, upper n strings are oriented from left to right and lower m strings are oriented from right to left. The properties of $\mathcal{S}(H_{n,m})$ is deeply investigated in [1], in which $\mathcal{S}(H_{n,m})$ is referred to as $H_{n-1,m-1}$. We construct an element of $\mathcal{S}(H_{n,m})$ denoted by $h_{n,m}$. First we inductively define $h_n = h_{n,0}$ in $\mathcal{S}(H_{n,0})$.

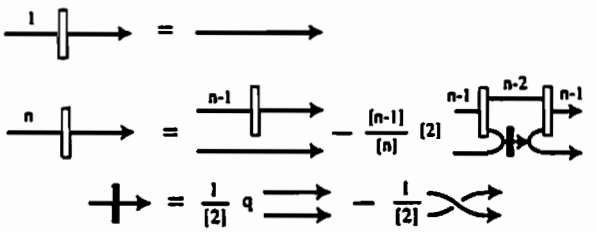


Figure 2: definition of $h_n = h_{n,0}$

Note that if we reflect $h_{n,0}$ vertically, we also get $h_{0,n}$ in $\mathcal{S}(B_{0,n})$.

Next lemma is one of well-known properties of $h_{n,0}$.

Lemma 1. *For any integer i ($0 \leq i \leq n-2$), we have*

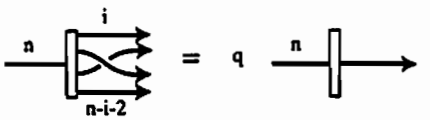


Figure 3: property of h_n

Next we inductively define $h_{n,m}$ in $\mathcal{S}(B_{n,m})$ by

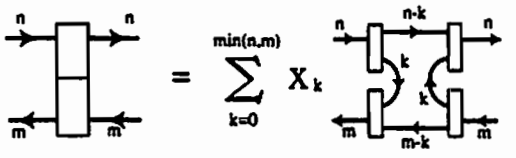


Figure 4: definition of $h_{n,m}$

where

$$x_k = (-1)^k \begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} m \\ k \end{bmatrix} \frac{[k]!}{[n+m-2]_a \cdots [n+m-k-1]_a}.$$

Next lemma is an elementary property of $h_{n,m}$.

Lemma 2. *The following holds.*

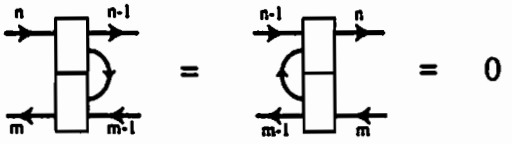
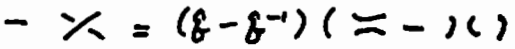


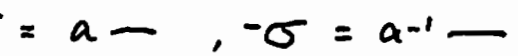
Figure 5: property of $h_{n,m}$

2.2 Kauffman case

We consider diagrams of unoriented links and n unoriented arcs on a surface F. There are $2n$ points $p_1, \ldots, p_n$ on the boundary of F and the terminals of the arcs are these n points. A complex vector space $\mathcal{S}(F) = \mathcal{S}(F, \{p_1, \ldots, p_n\})$ consists of formal linear sums of such diagrams quotiented by

(1) regular isotopy and $D \cup \bigcirc = ([0]_a + 1)\, D$

(2) 

(3) 

where D is any diagram in F and $\bigcirc$ is null-homotopic in F. We call the complex vector space $\mathcal{S}(F, \{p_1, \ldots, p_{2n}\})$ a linear skein associated with Kauffman polynomials. It is also well-known that if we take S^2 with no points as F, then $\mathcal{S}(S^2)$ is equal to $\mathbb{C}$ and if the diagram is only one link diagram with coefficient 1, the correspond complex value is the Kauffman polynomial of the link. As F, we consider a square with $2n$ points, n points are located on the left and right side and We denote this square with $2n$ points by K_n. On $\mathcal{S}(K_n)$, we can

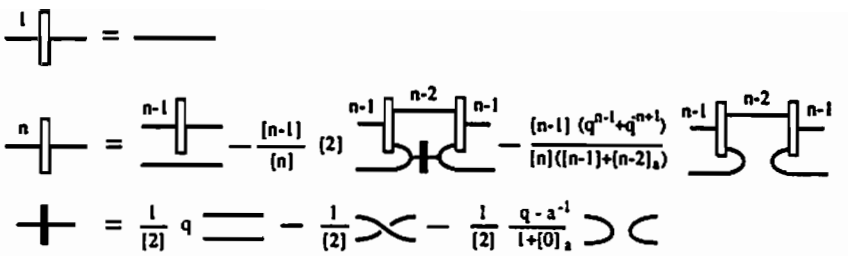


Figure 6: definition of k_n

define a multiplication by setting two elements left and right, and then connecting straightforwardly left n points with right n points. By this multiplication, $\mathcal{S}(K_n)$ become an algebra over $\mathbb{C}$. We denote the identity element by 1_n in $\mathcal{S}(K_n)$, which is straight $2n$ strings. We inductively define k_n in $\mathcal{S}(K_n)$ by Next lemma is one of well-known properties of k_n.

Lemma 3. *For any integer i ($0 \leq i \leq n-2$), we have*

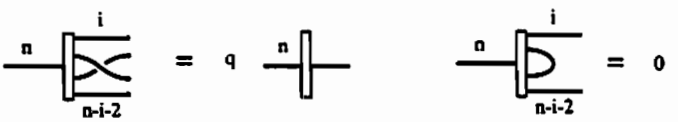


Figure 7: property of k_n

3 Construction of Invariants

In this sections, we construct invariants of trivalent graphs. At first, we prepare some propositions. Unless stated otherwise, when we consider oriented diagrams it means Homfly case, and when we consider unoriented diagrams it means Kauffman case. For a trivalent graph diagram G on S^2 and an even integer $2n$, we will induce a link diagram by replacing each edge by $2n$ strings and attaching $h_{n,n}$ or k_{2n} on each edge.

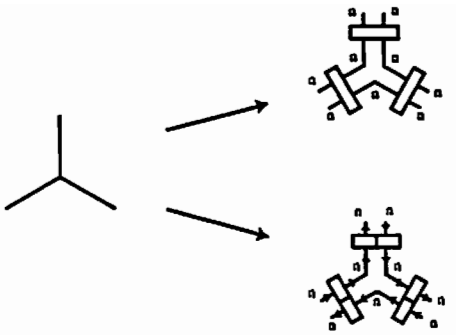


Figure 8: diagram around a vertex

We denote Homfly case by $R_{2n}(G)$ in $\mathcal{S}(S^2)$ and Kauffman case by $\Lambda_{2n}(G)$ in $\mathcal{S}(S^2)$. Then we have linear sums of oriented link diagrams on S^2, therefore we have two complex values.

Proposition 1. *We have* $R_{2n}(G_1) = a^{-n}q^{-n(n-1)}R_{2n}(G_2)$ *and* $\Lambda_{2n}(G_1) = a^{-n}q^{n}\Lambda_{2n}(G_2)$ *where*

Figure 9: G_1 and G_2

and resulting diagrams expect G_1 *and* G_2 *are same.*

We define a complex value $\Omega_{2n}(G)$ by $\{R_{2n}(G)\} \times \{\Lambda_{2n}(G!)|_{a\to aq^n}\}$ where $G!$ is the mirror image of G. Then we can show the complex value $\Omega_{2n}(G)$ are invariant under the moves.

Theorem 1. *For a trivalent graph diagram* G *on* S^2 *and an even integer* $2n$, *The complex value* $\Omega_{2n}(G)$ *is invariant under the moves. Therefore* $\Omega_{2n}(G)$ *is an invariant of trivalent graphs.*

We can extend $\Omega_{2n}(G)$ for any graph diagrams G (not necessarily trivalent). In this case, unfortunately $\Omega_{2n}(G)$ is not invariant under the move (V). Therefore

Corollary 1. *For a graph diagram* G *and an even integer* $2n$, $\Omega_{2n}(G)$ *is invariant under the moves (I),* $\cdots$, *(IV).*

References

[1] M. Kosuda, J. Murakami. Centralizer algebras of the mixed tensor representations of quantum group $U_q(\mathrm{gl}(n, \mathbf{C}))$. Osaka J. Math. 30 (1993), no. 3, 475–507.

[2] J. Murakami. The Yamada polynomial of spacial graphs and knit algebras. Comm. Math. Phys. 155 (1993), no. 3, 511–522.

[3] S. Yamada. An invariant of spatial graphs. J. Graph Theory 13 (1989), no. 5, 537–551.

[4] Y. Yokota. Topological invariants of graphs in 3-space. Topology 35 (1996), no. 1, 77–87.

切断点を持つ非標識連結グラフの数え上げ

金 應烈　　田澤新成　　白倉暉弘
神戸大学　　近畿大学　　神戸大学

ここでは、単純グラフ、すなわち多重辺とループを持たないグラフのみを扱うことにする。

唯1つの切断点を持つ標識連結グラフの数え上げは金、田澤、白倉 ([4]) によって得られた。また、非標識単純グラフについて、グラフの全体の巡回指数和は Robinson([3]) によって見出され、グラフの全体と連結グラフの全体とのそれぞれの巡回指数和の間の関係は Harary([2]) と Cadogan([1]) によって見出された。さらに、Robinson([3]) はブロックの巡回指数和の公式を与えた。ここでは、これらの巡回指数和から、唯1つの切断点を持つ非標識連結グラフの数え上げを述べる。

グラフ G の自己同型写像 α というのは、G の点集合 V の上の置換で、隣接性を保存するようなものである。G の自己同型写像の全体からなる置換群 $\Gamma(G)$ の巡回指数 $Z(\Gamma(G))$ を

$$Z(\Gamma(G)) = \frac{1}{|\Gamma(G)|} \sum_{\alpha \in \Gamma(G)} \prod_{k=1} s_k^{j_k(\alpha)} \tag{1}$$

で表す。ここで、s_k を長さ k の巡回とし、$j_k(\alpha)$ を $\Gamma(G)$ の元 α における長さ k の巡回成分の個数とする。

このとき、グラフ G の位数が p であれば、$1j_1(\alpha)+2j_2(\alpha)+\cdots+pj_p(\alpha)=p$ であり、$s_1=s_2=\cdots=1$ とおくと、$Z(\Gamma(G))=1$ である。

次に、$\mathcal{G}$ を同型でないグラフの全体とし、$\mathcal{G}$ の巡回指数和を $Z(\mathcal{G})=\sum_{G\in\mathcal{G}} Z(\Gamma(G))$ と定める。

このとき、次の命題が得られる。

命題 1 位数が p である同型でないグラフの全体 $\mathcal{G}_p$ における巡回指数和 $Z(\mathcal{G}_p)$ に $s_1=s_2=\cdots=s_p=1$ を代入すると、$\mathcal{G}_p$ の要素の個数になる。

S_n を対象集合 $X=\{1,2,\cdots,n\}$ の上の置換群とし、$S_n^{(2)}$ を X の2部集合からなる集合 $X^{(2)}$ の上の置換群とする。また、$S_n^{(1,2)}$ を対象集合 $X\cup X^{(2)}$ 上の置換群とすると、次の定理が知られている。

定理 2 非標識グラフの全体 $\mathcal{G}$ における巡回指数和 $Z(\mathcal{G})$ は

$$Z(\mathcal{G}) = \sum_{n=1}^{\infty} Z(S_n^{(1,2)}; s_k, 2) \tag{2}$$

で与えられる。

ここで、$j_k(\alpha)$ と $j_k(\alpha')$ をそれぞれ置換群 S_n と $S_n^{(2)}$ の元 α と α' における長さ k の巡回成分の個数とすると、

$$Z(S_n^{(1,2)}; s_k, 2) = \frac{1}{n!} \sum_{\alpha \in S_n} \prod_{k=1}^{\binom{n}{2}} 2^{j_k(\alpha')} \prod_{k=1}^{n} s_k^{j_k(\alpha)}$$

である。

定理 2 により、$Z(\mathcal{G})$ の最初のいくつかの項を計算すると、次のようになる。

$$\begin{aligned} Z(\mathcal{G}) &= s_1 + s_1^2 + s_2 + \frac{4}{3}s_1^3 + 2s_1s_2 + \frac{2}{3}s_3 + \frac{8}{3}s_1^4 + 4s_1^2s_2 + 2s_2^2 + \frac{4}{3}s_1s_3 + s_4 \\ &\quad + \frac{128}{15}s_1^5 + \frac{32}{3}s_1^3s_2 + \frac{8}{3}s_1^2s_3 + 8s_1s_2^2 + 2s_1s_4 + \frac{4}{3}s_2s_3 + \frac{4}{5}s_5 + \cdots. \end{aligned}$$

したがって、定理 2 と命題 1 により、$p = 1, 2, \cdots, 10$ について、位数が p である非標識グラフの個数 $|\mathcal{G}_p|$ を計算すると、次の表 1 のようになる.

表 1．位数が p であるグラフの個数

p	1	2	3	4	5	6	7	8	9	10
$\lvert\mathcal{G}_p\rvert$	1	2	4	11	34	156	1044	12346	274668	12005168

A を対象集合 $X = \{1, 2, \cdots, n\}$ 上の置換群とし、Y を同型でないグラフの集合とする。X から Y への写像 f, g に対し、ある $\alpha \in A$ に関し、$g = \alpha f$ であるとき、f と g は同値であるといい、写像の全体を同値関係で類別する。類の集合を $\mathfrak{F}$ と書く。このとき、次の定理が知られている。

定理 3 （合成定理）

$$Z(\mathfrak{F}) = Z(A)[\sum_{G \in Y} Z(\Gamma(G))] \tag{3}$$

ここで、$Z(A)[\sum_{G \in Y} Z(\Gamma(G))]$ は $Z(A)$ における各変数 s_k を

$$\sum_{G \in Y} Z(\Gamma(G); s_k, s_{2k}, s_{3k}, \cdots)$$

で置き換える。

定理 4 連結グラフの全体 $\mathcal{C}$ の巡回指数和 $Z(\mathcal{C})$ と $Z(\mathcal{G})$ との間に関係式

$$Z(\mathcal{C}) = \sum_{i=1}^{\infty} \frac{\mu(i)}{i} \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j} s_i^j [Z(\mathcal{G})] \tag{4}$$

が成り立つ。ここで、$\mu(i)$ はメービウス関数である。

定理 4 により、$Z(\mathcal{C})$ の最初のいくつかの項を計算すると、次のようになる。

$$\begin{aligned} Z(\mathcal{C}) &= s_1 + \frac{1}{2}s_1^2 + \frac{1}{2}s_2 + \frac{2}{3}s_1^3 + s_1s_2 + \frac{1}{3}s_3 + \frac{19}{12}s_1^4 + 2s_1^2s_2 + \frac{5}{4}s_2^2 + \frac{2}{3}s_1s_3 + \frac{1}{2}s_4 \\ &\quad + \frac{91}{15}s_1^5 + \frac{19}{3}s_1^3s_2 + \frac{4}{3}s_1^2s_3 + 5s_1s_2^2 + s_1s_4 + \frac{2}{3}s_2s_3 + \frac{3}{5}s_5 + \cdots. \end{aligned}$$

したがって、定理 4 と命題 1 により、$p = 1, 2, \cdots, 10$ について、位数が p である非標識連結グラフの個数 $|\mathcal{C}_p|$ を計算すると、次の表 2 のようになる.

表 2．位数が p である連結グラフの個数

p	1	2	3	4	5	6	7	8	9	10
$\lvert\mathcal{C}_p\rvert$	1	1	2	6	21	112	853	11117	261080	11716571

次に、ブロックの全体 $\mathcal{B}$ における巡回指数和を $Z(\mathcal{B})$ とする。また、根付き連結グラフの全体 C' の巡回指数和を $Z(C')$ とし、根付きブロックの全体 $\mathcal{B}'$ の巡回指数和を $Z(\mathcal{B}')$ とする。このとき、次のことが知られている。

$$Z(C') = \frac{\partial Z(C)}{\partial s_1}, \qquad Z(\mathcal{B}') = \frac{\partial Z(\mathcal{B})}{\partial s_1}.$$

定理 5 $Z(C')$ と $Z(\mathcal{B}')$ との間に関係式

$$Z(\mathcal{B}')[s_1 Z(C')] = \sum_{i=1}^{\infty} \frac{\mu(i)}{i} s_i[\log Z(C')] \tag{5}$$

が成り立つ。

命題 6 位数が p までであるブロック全体の巡回指数和を $Z(\mathcal{B}(p))$ とし、位数が p であるブロック全体の巡回指数和を $Z(\mathcal{B}_p)$ とする。このとき、次のことが成立する。

$$\begin{aligned} Z(\mathcal{B}(2))|_{s_1=0} &= \frac{1}{2}s_2, \\ Z(\mathcal{B}(2))[s_1 Z(C')]|_{s_1=0} &= Z(C)|_{s_1=0}, \\ Z(\mathcal{B}(p+1))[s_1 Z(C')]|_{s_1=0} &= Z(\mathcal{B}(p))[s_1 Z(C')]|_{s_1=0} - Z(\mathcal{B}_p)[s_1 Z(C')]|_{s_1=0}. \end{aligned}$$

定理 7 ブロック全体の巡回指数和は

$$Z(\mathcal{B}) = \int_0^{s_1} Z(\mathcal{B}')ds_1 + Z(\mathcal{B})|_{s_1=0} \tag{6}$$

によって与えられる。

定理 5, 7 と命題 6 により、$Z(\mathcal{B})$ の最初のいくつかの項を計算すると、次のようになる。

$$Z(\mathcal{B}) = \frac{1}{2}s_1^2 + \frac{1}{2}s_2 + \frac{1}{6}s_1^3 + \frac{1}{2}s_1 s_2 + \frac{1}{3}s_3 + \frac{5}{12}s_1^4 + s_1^2 s_2 + \frac{3}{4}s_2^2 + \frac{1}{3}s_1 s_3 + \frac{1}{2}s_4 + \cdots.$$

したがって、命題 1 により、$p = 1, 2, \cdots, 9$ について、位数が p である非標識ブロックの個数 $|\mathcal{B}_p|$ を計算すると、次の表 3 のようになる.

表 3. 位数が p であるブロックの個数

p	1	2	3	4	5	6	7	8	9
$\lvert\mathcal{B}_p\rvert$	0	1	1	3	10	56	468	7123	194066

$\mathcal{V}_1'$ を唯一つの切断点を根とする根付き連結グラフの全体とし、その巡回指数和を $Z(\mathcal{V}_1')$ で表す。このとき、合成定理により、次の定理を得る。

定理 8

$$Z(\mathcal{V}_1') = \exp\{\sum_{k=1}^{\infty} \frac{s_k}{k}[Z(\mathcal{B}')]\} - (1 + Z(\mathcal{B}')). \tag{7}$$

A, B をそれぞれ互いに素な有限集合 X と Y 上の置換群とし、AB を和集合 $X \cup Y$ 上の置換群とする。ここで、AB の各置換は X 上の置換 α と Y 上の置換 β の積で表されているものとする。つまり $z \in X \cup Y$ は AB の置換 $\alpha\beta$ によって次のように置換される。

$$(\alpha\beta)z = \begin{cases} \alpha z. & z \in X. \\ \beta z. & z \in Y. \end{cases}$$

このとき、次のことが知られている。

命題 9 AB の巡回指数は

$$Z(AB) = Z(A)Z(B) \tag{8}$$

によって与えられる。

最後に、$\mathcal{V}_1$ を唯一つの切断点を持つ連結グラフの全体とし、その巡回指数和を $Z(\mathcal{V}_1)$ で表す。このとき、命題 9 と定理 8 より、次の定理を得る。

定理 10 $Z(\mathcal{V}_1)$ と $Z(\mathcal{B}')$ との間に関係式

$$Z(\mathcal{V}_1) = s_1 \cdot \exp\{\sum_{k=1}^{\infty} \frac{s_k}{k}[Z(\mathcal{B}')]\} - (s_1 + s_1 \cdot Z(\mathcal{B}')) \tag{9}$$

が成立する。

定理 10 により、$Z(\mathcal{V}_1)$ の最初のいくつかの項を計算すると、次のようになる。

$$\begin{aligned} Z(\mathcal{V}_1) \;=\; & \frac{1}{2}s_1^3 + \frac{1}{2}s_1 s_2 + \frac{2}{3}s_1^4 + s_1^2 s_2 + \frac{1}{3}s_1 s_3 + \frac{25}{12}s_1^5 + 3s_1^3 s_2 + \frac{3}{4}s_1 s_2^2 + \frac{2}{3}s_1^2 s_3 + \frac{1}{2}s_1 s_4 \\ & + \frac{59}{5}s_1^6 + \frac{34}{3}s_1^4 s_2 + 2s_1^3 s_3 + 6s_1^2 s_2^2 + s_1^2 s_4 + \frac{2}{3}s_1 s_2 s_3 + \frac{1}{5}s_1 s_5 + \cdots. \end{aligned}$$

ゆえに、命題 1 により、$p = 1, 2, \cdots, 10$ について、唯 1 つの切断点をもつ位数が p である非標識連結グラフの個数 $|\mathcal{V}_{1,p}|$ を計算すると、次の表 4 のようになる.

表 4. 唯 1 つの切断点をもつ連結グラフの個数

p	1	2	3	4	5	6	7	8	9	10
$\lvert\mathcal{V}_{1,p}\rvert$	0	0	1	2	7	33	244	2792	52448	1690206

参考文献

[1] C.C. Cadogan, *The möbius function and connected graphs*. J. Combinatorial Theory,11B(1971), 193-200.

[2] F. Harary, *The number of linear, directed, rooted, and connected graphs*. Trans. Amer. Math. Soc. 78(1955), 445-463.

[3] Robinson, R. W. *Enumeration of non-separable graphs*. J. Combinatorial Theory,9(1970), 327-356.

[4] 金　應烈, 田澤　新成, 白倉暉弘, *Enumeration of lablled connected graphs with only one cut vertex*. 離散幾何・組合せ論ワークショップ (琉球大学), 1997.

Cyclic resolutions of the BIB design associated with $PG(7,2)$ and $PG(5,2)$

菱田 隆彰
岐阜大学大学院工学研究科電子情報システム工学専攻

A pair $(\mathcal{V}, \mathcal{B})$ is called a *BIB design* if $\mathcal{V}$ is a set of v *points* and $\mathcal{B}$ is a collention of b k-subsets of $\mathcal{V}$ (called *blocks*) such that every pair of points is contained in exactly λ blocks.

For a BIB design $(\mathcal{V}, \mathcal{B})$, let σ be a permutation on $\mathcal{V}$. If $\mathcal{B}^\sigma = \{B^\sigma | B \in \mathcal{B}\} = \mathcal{B}$ then σ is called an *automorphism* of $(\mathcal{V}, \mathcal{B})$, where $B^\sigma = \{b_1^\sigma, b_2^\sigma, \ldots, b_k^\sigma\}$ for any $B = \{b_1, b_2, \ldots, b_k\} \in \mathcal{B}$. If an automorphism σ of $(\mathcal{V}, \mathcal{B})$ have a cycle of length v, the design is called *cyclic*.

For a cyclic BIB design, we can identify $\mathcal{V}$ with $Z_v = \{0, 1, \ldots, v-1\}$ (mod v). In this case $\sigma : x \mapsto x+1$ (mod v) and $B^\sigma = B + 1 = \{b_1 + 1, b_2 + 1, \ldots, b_k + 1\}$ (mod v). And the *block orbit* containing $B = \{b_1, b_2, \ldots, b_k\}$ is defined by the set of distinct blocks $B^{\sigma^i} = B + i = \{b_1 + i, b_2 + i, \ldots, b_k + i\}$ (mod v) for $i \in Z_v$.

If R is a set of blocks such that every point of $\mathcal{V}$ is contained exactly one block in R, then R is called a *resolution class*. If the set of blocks in a BIB design $(\mathcal{V}, \mathcal{B})$ is partitioned into resolution classes $R_1, R_2, \ldots, R_d$ then the design is called *resolvable*. And $\mathcal{R} = \{R_1, R_2, \ldots, R_d\}$ is called a *resolution*.

Assume that a cyclic BIB design $(\mathcal{V}, \mathcal{B})$ is resolvable and let $\mathcal{R} = \{R_1, R_2, \ldots, R_d\}$ be a set of resolution classes of $(\mathcal{V}, \mathcal{B})$. For a resolution class R_i, let $R_i + 1 = \{B + 1 \pmod v | B \in R_i\}$, and $\mathcal{R} + 1 = \{R_1 + 1, R_2 + 1, \ldots, R_d + 1\}$. If $\mathcal{R} + 1 = \{R_1 + 1, R_2 + 1, \ldots, R_d + 1\} = \mathcal{R}$ then the design is called *cyclically resolvable*. In the sequel, we denote a cyclically resolvable cyclic BIB design with parameters v, k, λ by CRCB(v, k, λ).

The notion of a CRCB was first introduced by Genma, Mishima and Jimbo (1997). The notion of a CRCB is useful not only in the field of the statistical design of experiments but also in the field of cryptography. In cryptography, a CRCB is utilized to construct a secret sharing scheme. On the other hand, it is well known that the incidence relation of points and lines in $PG(n, q)$ is a BIB design with parameters $v = \frac{q^{n+1}-1}{q-1}$, $k = q + 1$, $\lambda = 1$.

Beutelspacher (1974) showed the existence of a resolution in $PG(2^i - 1, q)$ for $i \geq 2$. Baker (1976) and Wettl (1991) gave constructions of resolutions in $PG(2m+1, 2)$ for any positive integer m, whose automorphism is not cyclic on the points. Recently, Sarmiento (1997) showed that the BIB design consisting of points and lines in $PG(5, 2)$ was cyclically resolvable by using computer, and enumerated all inequivalent resolutions.

Here, we show the following:

Proposition 1. Cyclic BIB designs generated by points and lines in $PG(7, 2)$ are cyclically resolvable.

As far as we know no resolution of BIB designs generated by planes (or higher flats) and points are known. For this regards, we obtain the following:

Proposition 2. Cyclic BIB designs generated by points and planes in $PG(5, 2)$ are cyclically resolvable.

The above results were obtained by using computer.

Balanced bipartite block design の構成法について

三嶋 美和子　岐阜大・工

Let V_1 be a set of v_1 points with r_1 replicates, V_2 be another set of v_2 points with r_2 replicates and $\mathcal{B}$ be a collection of k-subsets called a *block* (*superblock*) of $V_1 \cup V_2$. An incomplete block binary design $(V_1, V_2, \mathcal{B})$ is called a *balanced bipartite block design* if

(i) any two distinct points of V_i occur together in λ_{ii} blocks, $i = 1, 2$;

(ii) any two distinct points from different sets occur together in $\lambda_{12} = \lambda_{21}$ blocks.

Here, we focus on a special type of balanced bipartite block designs which satisfies the following additional condition:

(iii) each superblock of $\mathcal{B}$ is divided into a k_1-subset of V_1 and a k_2-subset of V_2.

The following two theorems are constructions for this type of balanced bipartite block designs.

Theorem 1. *Let $n \geq 3$ be an integer and q be a prime power. Then there exists a balanced bipartite block design with parameters*

$$v_1 = v_2 = q^{n-1}, \quad b = \frac{q^2(q^{n-1}-1)}{q-1}, \quad r_1 = r_2 = \frac{q(q^{n-1}-1)}{q-1},$$

$$k_1 = k_2 = q^{n-2}, \quad \lambda_{11} = \lambda_{22} = \lambda_{12} - 1 = \frac{q^{n-1}-1}{q-1} - 1.$$

Theorem 2. *The existence of two designs, i.e.* (i) *a BIB design with parameters v_1, b_1', r_1', k_1, λ_1', and* (ii) *an α-resolvable BIB design with parameters v_2, b_2', r_2', k_2, λ_2', implies the existence of a balanced bipartite block design with parameters*

$$v_1, \quad v_2, \quad b = c_1 b_1' = c_2 b_2', \quad r_1 = c_1 r_1', \quad r_2 = c_2 r_2',$$

$$k_1, \quad k_2, \quad \lambda_{11} = c_1 \lambda_1', \quad \lambda_{22} = c_2 \lambda_2', \quad \lambda_{12} = \frac{k_1 k_2}{v_1 v_2} b,$$

where $c_1 = b_2'/\gcd(b_1', r_2'/\alpha)$ and $c_2 = b_1'/\gcd(b_1', r_2'/\alpha)$.

A lower bound of the number of superblocks is as follows.

Theorem 3. *If there exists a balanced bipartite block design with parameters v_1, v_2, b, r_1, r_2, k_1, k_2, λ_{11}, λ_{22}, λ_{12}, then*

$$\frac{4}{d_1 d_2 d_3} \binom{v_1}{2} \binom{v_2}{2} \Big| b \tag{1}$$

holds, that is, the left-hand side of (1) *is a lower bound of b, where*

$$d_1 = \gcd(k_2(v_1-1), (k_1-1)v_2), \quad d_2 = \gcd(k_1(v_2-1), (k_2-1)v_1),$$
$$d_3 = \gcd\left(\frac{k_2(v_1-1)}{d_1}, \frac{k_1(v_2-1)}{d_2}\right) \tag{2}$$

For each of the resulting designs of Theorems 1 and 2, we will derive a sufficient condition for the number of superblocks to attain the lower bound given in Theorem 3.

Theorem 4. *In a balanced bipartite block design having the same parameters as the design of Theorem 1, the number of superblocks attains the lower bound of Theorem 3.*

Theorem 5. *Assume that there exists a balanced bipartite block design having the same parameters as the design of Theorem 2, and that*

$$\lambda_2' \Big| \frac{k_2(k_2-1)v_1(v_1-1)}{d_1 d_2 d_3} \quad \text{and} \quad \frac{\alpha v_2 \lambda_1'}{k_2} \Big| \frac{k_1(k_1-1)v_2(v_2-1)}{d_1 d_2 d_3}.$$

Then the number of superblocks attains the lower bound of Theorem 3, if

$$\gcd\left(\frac{(k_2-1)v_1}{d_2}, \frac{(k_1-1)v_2}{d_1}\right) = \frac{1}{m} \gcd\left(\frac{(k_2-1)v_1}{d_2}, \frac{\alpha v_2 \lambda_1'}{k_2}\right) \cdot \gcd\left(\frac{(k_1-1)v_2}{d_1}, \lambda_2'\right)$$

holds, where $m = \gcd(\lambda_2', \alpha v_2 \lambda_1'/k_2)$, and d_1, d_2 and d_3 are defined by (2).

$\tilde{S}_k$ - factorization of symmetric complete tripartite digraphs

Kazuhiko Ushio
Department of Industrial Engineering
Faculty of Science and Technology
Kinki University
Osaka 577-8502, JAPAN
E-mail:ushio@is.kindai.ac.jp

Abstract

We show that a necessary and sufficient condition for the existence of an $\tilde{S}_k$ - factorization of the symmetric complete tripartite digraph $K^*_{n_1,n_2,n_3}$ is (i) k is even, $k \geq 4$ and (ii) $n_1 = n_2 = n_3 \equiv 0 \pmod{k(k-1)/3}$ for $k \equiv 0 \pmod 6$ and $n_1 = n_2 = n_3 \equiv 0 \pmod{k(k-1)}$ for $k \equiv 2, 4 \pmod 6$.

Keywords: Star-factorization, Symmetric complete tripartite digraph

1. Introduction

Let $K^*_{n_1,n_2,n_3}$ denote *the symmetric complete tripartite digraph* with partite sets V_1, V_2, V_3 of n_1, n_2, n_3 vertices each, and let $\tilde{S}_k$ denote *the semi-evenly partite directed star* from a center-vertex to $k-1$ end-vertices such that the center-vertex is in V_i and $(k-2)/2$ end-vertices are in V_{j_1} and $k/2$ end-vertices are in V_{j_2} with $\{i, j_1, j_2\}=\{1,2,3\}$. A spanning subgraph F of $K^*_{n_1,n_2,n_3}$ is called an $\tilde{S}_k$ - *factor* if each component of F is $\tilde{S}_k$. If $K^*_{n_1,n_2,n_3}$ is expressed as an arc-disjoint sum of $\tilde{S}_k$ - factors, then this sum is called an $\tilde{S}_k$ - *factorization* of $K^*_{n_1,n_2,n_3}$.
In this paper, it is shown that a necessary and sufficient condition for the existence of such a factorization is (i) k is even, $k \geq 4$ and (ii) $n_1 = n_2 = n_3 \equiv 0 \pmod{k(k-1)/3}$ for $k \equiv 0 \pmod 6$ and $n_1 = n_2 = n_3 \equiv 0 \pmod{k(k-1)}$ for $k \equiv 2, 4 \pmod 6$.

Let K_{n_1,n_2}, $K^*_{n_1,n_2}$, $K^*_{n_1,n_2,n_3}$, and $K^*_{n_1,n_2,\ldots,n_m}$ denote the complete bipartite graph, the symmetric complete bipartite digraph, the symmetric complete tripartite digraph, and the symmetric complete multipartite digraph, respectively. And let $\dot{C}_k$, $\dot{S}_k$, $\dot{P}_k$, and $\dot{K}_{p,q}$ denote the cycle or the directed cycle, the star or the directed star, the path or the directed path, and the complete bipartite graph or the complete bipartite digraph, respectively, on two partite sets V_i and V_j. Then the problems of giving the necessary and sufficient conditions of $\dot{C}_k$ - factorization of K_{n_1,n_2}, $K^*_{n_1,n_2}$, and $K^*_{n_1,n_2,n_3}$ have been completely solved by Enomoto, Miyamoto and Ushio[2] and Ushio[12]. $\dot{S}_k$ - factorization of K_{n_1,n_2}, $K^*_{n_1,n_2}$, and $K^*_{n_1,n_2,n_3}$ have been studied by Ushio and Tsuruno[8], Ushio[13], and Wang[14]. Recently, Martin[4,5] and Ushio[10] give the necessary and sufficient conditions of $\dot{S}_k$ - factorization of K_{n_1,n_2} and $K^*_{n_1,n_2}$. $\dot{P}_k$ - factorization of K_{n_1,n_2} and $K^*_{n_1,n_2}$ have been studied by Ushio and Tsuruno[7], and Ushio[6,9]. $\dot{K}_{p,q}$ - factorization of K_{n_1,n_2} has been studied by Martin[4]. Ushio[11] gives the necessary and sufficient condition of $\dot{K}_{p,q}$ - factorization of $K^*_{n_1,n_2}$. For graph theoretical terms, see [1,3].

2. $\tilde{S}_k$ - factorization of $K^*_{n_1,n_2,n_3}$

Notation. Given an $\tilde{S}_k$ - factorization of $K^*_{n_1,n_2,n_3}$, let
r be the number of factors
t be the number of components of each factor

Department of Industrial Engineering, Faculty of Science and Technology, Kinki University, Osaka 577-8502, JAPAN. E-mail:ushio@is.kindai.ac.jp

b be the total number of components.
Among r components having vertex x in V_i, let r_{ij} be the number of components whose center-vertex is in V_j .

Theorem 1. If $K^*_{n_1,n_2,n_3}$ has an $\tilde{S}_k$ - factorization, then (i) k is even, $k \geq 4$ and (ii) $n_1 = n_2 = n_3 \equiv 0 \pmod{k(k-1)/3}$ for $k \equiv 0 \pmod 6$ and $n_1 = n_2 = n_3 \equiv 0 \pmod{k(k-1)}$ for $k \equiv 2, 4 \pmod 6$.

Proof. Suppose that $K^*_{n_1,n_2,n_3}$ has an $\tilde{S}_k$ - factorization. Then $b = 2(n_1n_2+n_1n_3+n_2n_3)/(k-1)$, $t = (n_1+n_2+n_3)/k$, $r = b/t = 2(n_1n_2+n_1n_3+n_2n_3)k/(n_1+n_2+n_3)(k-1)$. By the definition of $\tilde{S}_k$, k is even and $k \geq 4$.
For a vertex x in V_1, we have $r_{11}(k-1) = n_2 + n_3$, $r_{12} = n_2$, $r_{13} = n_3$, and $r_{11} + r_{12} + r_{13} = r$.
For a vertex x in V_2, we have $r_{22}(k-1) = n_1 + n_3$, $r_{21} = n_1$, $r_{23} = n_3$, and $r_{21} + r_{22} + r_{23} = r$.
For a vertex x in V_3, we have $r_{33}(k-1) = n_1 + n_2$, $r_{31} = n_1$, $r_{32} = n_2$, and $r_{31} + r_{32} + r_{33} = r$.
Therefore, we have $n_1 = n_2 = n_3$. Put $n_1 = n_2 = n_3 = n$. Then $r_{11} = r_{22} = r_{33} = 2n/(k-1)$, $r_{12} = r_{13} = r_{21} = r_{23} = r_{31} = r_{32} = n$, $b = 6n^2/(k-1)$, $t = 3n/k$, $r = 2nk/(k-1)$.
Since k is even and $k \geq 4$, we must have $3n \equiv 0 \pmod k$ and $n \equiv 0 \pmod{k-1}$. Therefore, we have $n \equiv 0 \pmod{k(k-1)/3}$ for $k \equiv 0 \pmod 6$ and $n \equiv 0 \pmod{k(k-1)}$ for $k \equiv 2, 4 \pmod 6$.

Theorem 2. If $K^*_{n,n,n}$ has an $\tilde{S}_k$ - factorization, then $K^*_{sn,sn,sn}$ has an $\tilde{S}_k$ - factorization.

Proof. Let $K_{q_1,q_2\oplus q_3}$ denote the tripartite digraph with partite sets U_1, U_2, U_3 of q_1, q_2, q_3 vertices such that q_1 start-vertices in U_1 are adjacent to both q_2 end-vertices in U_2 and q_3 end-vertices in U_3. Then $\tilde{S}_k$ can be denoted by $K_{1,a\oplus(a+1)}$ for $k = 2a+2$. When $K^*_{n,n,n}$ has an $\tilde{S}_k$ - factorization, $K^*_{sn,sn,sn}$ has a $K_{s,sa\oplus s(a+1)}$ - factorization. $K_{s,sa\oplus s(a+1)}$ has an $\tilde{S}_k$ - factorization. Therefore, $K^*_{sn,sn,sn}$ has an $\tilde{S}_k$ - factorization.

Theorem 3. When k is even, $k \geq 4$ and $n \equiv 0 \pmod{k(k-1)}$, $K^*_{n,n,n}$ has an $\tilde{S}_k$ - factorization.

Proof. Put $n = k(k-1)s$, $N = k(k-1)$. When $s = 1$, let $V_1 = \{1, 2, ..., N\}$, $V_2 = \{1', 2', ..., N'\}$, $V_3 = \{1'', 2'', ..., N''\}$. For $i = 1, 2, ..., k$ and $j = 1, 2, ..., k$, construct $2k^2$ $\tilde{S}_k$ - factors $F^{(1)}_{ij}$, $F^{(2)}_{ij}$ as following:

$F^{(1)}_{ij} = \{$ $((A+1);(B+(k-1)+1, ..., B+(k-1)+(k-2)/2)', (C+(k-1)+(k-2)/2+1, ..., C+2(k-1))'')$
$((A+2);(B+2(k-1)+1, ..., B+2(k-1)+(k-2)/2)', (C+2(k-1)+(k-2)/2+1, ..., C+3(k-1))'')$
...
$((A+k-1);(B+(k-1)^2+1, ..., B+(k-1)^2+(k-2)/2)', (C+(k-1)^2+(k-2)/2+1, ..., C+k(k-1))'')$
$((B+1)';(C+(k-1)+1, ..., C+(k-1)+(k-2)/2)'', (A+(k-1)+(k-2)/2+1, ..., A+2(k-1)))$
$((B+2)';(C+2(k-1)+1, ..., C+2(k-1)+(k-2)/2)'', (A+2(k-1)+(k-2)/2+1, ..., A+3(k-1)))$
...
$((B+k-1)';(C+(k-1)^2+1, ..., C+(k-1)^2+(k-2)/2)'', (A+(k-1)^2+(k-2)/2+1, ..., A+k(k-1)))$
$((C+1)'';(A+(k-1)+1, ..., A+(k-1)+(k-2)/2), (B+(k-1)+(k-2)/2+1, ..., B+2(k-1))')$
$((C+2)'';(A+2(k-1)+1, ..., A+2(k-1)+(k-2)/2), (B+2(k-1)+(k-2)/2+1, ..., B+3(k-1))')$
...
$((C+k-1)'';(A+(k-1)^2+1, ..., A+(k-1)^2+(k-2)/2), (B+(k-1)^2+(k-2)/2+1, ..., B+k(k-1))') \}$,

$F^{(2)}_{ij} = \{$ $((A+1);(C+(k-1)+1, ..., C+(k-1)+(k-2)/2)'', (B+(k-1)+(k-2)/2+1, ..., B+2(k-1))')$
$((A+2);(C+2(k-1)+1, ..., C+2(k-1)+(k-2)/2)'', (B+2(k-1)+(k-2)/2+1, ..., B+3(k-1))')$
...
$((A+k-1);(C+(k-1)^2+1, ..., C+(k-1)^2+(k-2)/2)'', (B+(k-1)^2+(k-2)/2+1, ..., B+k(k-1))')$
$((B+1)';(A+(k-1)+1, ..., A+(k-1)+(k-2)/2), (C+(k-1)+(k-2)/2+1, ..., C+2(k-1))'')$
$((B+2)';(A+2(k-1)+1, ..., A+2(k-1)+(k-2)/2), (C+2(k-1)+(k-2)/2+1, ..., C+3(k-1))'')$
...

$((B+k-1)';(A+(k-1)^2+1,...,A+(k-1)^2+(k-2)/2),(C+(k-1)^2+(k-2)/2+1,...,C+k(k-1))'')$
$((C+1)'';(B+(k-1)+1,...,B+(k-1)+(k-2)/2)',(A+(k-1)+(k-2)/2+1,...,A+2(k-1)))$
$((C+2)'';(B+2(k-1)+1,...,B+2(k-1)+(k-2)/2)',(A+2(k-1)+(k-2)/2+1,...,A+3(k-1)))$
...
$((C+k-1)'';(B+(k-1)^2+1,...,B+(k-1)^2+(k-2)/2)',(A+(k-1)^2+(k-2)/2+1,...,A+k(k-1)))\}$,
where $A=(i-1)(k-1)$, $B=(j-1)(k-1)$, $C=(i+j-2)(k-1)$, and the additions are taken modulo N with residues $1,2,...,N$.
Then we claim that they comprise an $\tilde{S}_k$ - factorization of $K^*_{N,N,N}$.
We can see that each of them is an $\tilde{S}_k$ - factor, because it spans all vertices of $K^*_{N,N,N}$. We show that they are arc-disjoint.
Suppose that they are not arc-disjoint. In the followings, we consider $A=(i-1)(k-1)$, $B=(j-1)(k-1)$, $C=(i+j-2)(k-1)$, $D=(h-1)(k-1)$, $E=(l-1)(k-1)$, $F=(h+l-2)(k-1)$, $1\le i,j,h,l\le k$. Note that A, B, C, D, E, F, N are integral multiples of $k-1$.
Let (X,Y') be an arc joining from V_1 to V_2 and let x and y be the residues of X and Y modulo $k-1$, respectively. Then the arc (X,Y') can appear only in the x-th components of $F^{(1)}_{ij}, F^{(2)}_{hl}$ according as $1\le y\le (k-2)/2, (k-2)/2+1\le y\le k-1$, respectively.
First, we assume that the common arc joining from V_1 to V_2 appears in x-th component $((A+x);(B+x(k-1)+1,...,B+x(k-1)+(k-2)/2)',(C+x(k-1)+(k-2)/2+1,...,C+(x+1)(k-1))'')$ of $F^{(1)}_{ij}$ and x-th component $((D+x);(E+x(k-1)+1,...,E+x(k-1)+(k-2)/2)',(F+x(k-1)+(k-2)/2+1,...,F+(x+1)(k-1))'')$ of $F^{(1)}_{hl}$.
Say $((A+x),(B+x(k-1)+y)')=((D+x),(E+x(k-1)+y)')$, where $1\le y\le (k-2)/2$.
Then $A+x\equiv D+x \pmod N$ and $B+x(k-1)+y\equiv E+x(k-1)+y \pmod N$. From the congruences, we have $A=D$ and $B=E$, which implies $i=h$ and $j=l$. This contradicts the assumption.
Next, we assume that the common arc joining from V_1 to V_2 appears in x-th component $((A+x);(C+x(k-1)+1,...,C+x(k-1)+(k-2)/2)'',(B+x(k-1)+(k-2)/2+1,...,B+(x+1)(k-1))')$ of $F^{(2)}_{ij}$ and x-th component $((D+x);(F+x(k-1)+1,...,F+x(k-1)+(k-2)/2)'',(E+x(k-1)+(k-2)/2+1,...,E+(x+1)(k-1))'')$ of $F^{(2)}_{hl}$.
Say $((A+x),(B+x(k-1)+y)')=((D+x),(E+x(k-1)+y)')$, where $(k-2)/2+1\le y\le k-1$.
Then $A+x\equiv D+x \pmod N$ and $B+x(k-1)+y\equiv E+x(k-1)+y \pmod N$. From the congruences, we have $A=D$ and $B=E$, which implies $i=h$ and $j=l$. This contradicts the assumption.
Thus, there is no common arc joining from V_1 to V_2.
Similarly, there are no common arcs joining from V_1 to V_3, from V_2 to V_1, from V_2 to V_3, from V_3 to V_1, or from V_3 to V_2.
Therefore, $2k^2$ $\tilde{S}_k$ - factors $F^{(1)}_{ij}$, $F^{(2)}_{ij}$ comprise an $\tilde{S}_k$ - factorization of $K^*_{N,N,N}$. Applying Theorem 2, $K^*_{n,n,n}$ has an $\tilde{S}_k$ - factorization.

Theorem 4. When $k\equiv 0 \pmod 6$ and $n\equiv 0 \pmod{k(k-1)/3}$, $K^*_{n,n,n}$ has an $\tilde{S}_k$ - factorization.

Proof. Put $k=6p$, $n=2p(6p-1)s$, $N=2p(6p-1)$. When $s=1$, let $V_1=\{1,2,...,N\}$, $V_2=\{1',2',...,N'\}$, $V_3=\{1'',2'',...,N''\}$. For $i=1,2,...,2p$ and $j=1,2,...,2p$, construct $24p^2$ $\tilde{S}_k$ - factors $F^{(1)}_{ij}$, $F^{(2)}_{ij}$, $F^{(3)}_{ij}$, $F^{(4)}_{ij}$, $F^{(5)}_{ij}$, $F^{(6)}_{ij}$ as following:

$F^{(1)}_{ij}=\{((A+1);(B+6p^2+5p-1,B+6p^2+5p-2,...,B+6p^2+2p+1)',(C+6p,C+6p+1,...,C+9p-1)'')$
$((A+2);(B+6p^2+2p,B+6p^2+2p-1,...,B+6p^2-p+2)',(C+9p,C+9p+1,...,C+12p-1)'')$
...
$((A+2p);(B+10p-2,B+10p-3,...,B+7p)',(C+6p^2+3p,C+6p^2+3p+1,...,C+6p^2+6p-1)'')$
$((B+2p+1)';(C+6p^2+6p,C+6p^2+6p+1,...,C+6p^2+9p-2)'',(A+6p^2,A+6p^2-1,...,A+6p^2-3p+1))$
$((B+2p+2)';(C+6p^2+9p-1,C+6p^2+9p,...,C+6p^2+12p-3)'',(A+6p^2-3p,A+6p^2-3p-1,...,A+6p^2-6p+1))$

...
$((B+3p)';(C+9p^2+2p+1, C+9p^2+2p+2, ..., C+9p^2+5p-1)'', (A+3p^2+3p, A+3p^2+3p-1, ..., A+3p^2+1))$
$((B+3p+1)';(C+9p^2+5p, C+9p^2+5p+1, ..., C+9p^2+8p-1)'', (A+3p^2, A+3p^2-1, ..., A+3p^2-3p+2))$
$((B+3p+2)';(C+9p^2+8p, C+9p^2+8p+1, ..., C+9p^2+11p-1)'', (A+3p^2-3p+1, A+3p^2-3p, ..., A+3p^2-6p+3))$
...
$((B+4p-1)';(C+12p^2-p, C+12p^2-p+1, ..., C+12p^2+2p-1)'', (A+7p-2, A+7p-3, ..., A+4p))$
$((C+4p)'';(A+6p^2+1, A+6p^2+2, ..., A+6p^2+3p-1), (B+4p, B+4p+1, ..., B+7p-1)')$
$((C+4p+1)'';(A+12p^2-2p, A+12p^2-2p-1, ..., A+12p^2-5p+1), (B+6p^2+5p, B+6p^2+5p+1, ..., B+6p^2+8p-2)')$
$((C+4p+2)'';(A+12p^2-5p, A+12p^2-5p-1, ..., A+12p^2-8p+1), (B+6p^2+8p-1, B+6p^2+8p, ..., B+6p^2+11p-3)')$
...
$((C+6p-2)'';(A+6p^2+7p, A+6p^2+7p-1, ..., A+6p^2+4p+1), (B+12p^2-6p+3, B+12p^2-6p+4, ..., B+12p^2-3p+1)')$
$((C+6p-1)'';(A+2p+1, A+2p+2, ..., A+4p-1, A+6p^2+3p, A+6p^2+3p+1, ..., A+6p^2+4p), (B+12p^2-3p+2, B+12p^2-3p+3, ..., B+12p^2)')$ },

$F_{ij}^{(2)} = \{ ((B+1)';(C+6p^2+5p-1, C+6p^2+5p-2, ..., C+6p^2+2p+1)'', (A+6p, A+6p+1, ..., A+9p-1))$
$((B+2)';(C+6p^2+2p, C+6p^2+2p-1, ..., C+6p^2-p+2)'', (A+9p, A+9p+1, ..., A+12p-1))$
...
$((B+2p)';(C+10p-2, C+10p-3, ..., C+7p)'', (A+6p^2+3p, A+6p^2+3p+1, ..., A+6p^2+6p-1))$
$((C+2p+1)'';(A+6p^2+6p, A+6p^2+6p+1, ..., A+6p^2+9p-2), (B+6p^2, B+6p^2-1, ..., B+6p^2-3p+1)')$
$((C+2p+2)'';(A+6p^2+9p-1, A+6p^2+9p, ..., A+6p^2+12p-3), (B+6p^2-3p, B+6p^2-3p-1, ..., B+6p^2-6p+1)')$
...
$((C+3p)'';(A+9p^2+2p+1, A+9p^2+2p+2, ..., A+9p^2+5p-1), (B+3p^2+3p, B+3p^2+3p-1, ..., B+3p^2+1)')$
$((C+3p+1)'';(A+9p^2+5p, A+9p^2+5p+1, ..., A+9p^2+8p-1), (B+3p^2, B+3p^2-1, ..., B+3p^2-3p+2)')$
$((C+3p+2)'';(A+9p^2+8p, A+9p^2+8p+1, ..., A+9p^2+11p-1), (B+3p^2-3p+1, B+3p^2-3p, ..., B+3p^2-6p+3)')$
...
$((C+4p-1)'';(A+12p^2-p, A+12p^2-p+1, ..., A+12p^2+2p-1), (B+7p-2, B+7p-3, ..., B+4p)')$
$((A+4p);(B+6p^2+1, B+6p^2+2, ..., B+6p^2+3p-1)', (C+4p, C+4p+1, ..., C+7p-1)'')$
$((A+4p+1);(B+12p^2-2p, B+12p^2-2p-1, ..., B+12p^2-5p+1)', (C+6p^2+5p, C+6p^2+5p+1, ..., C+6p^2+8p-2)'')$
$((A+4p+2);(B+12p^2-5p, B+12p^2-5p-1, ..., B+12p^2-8p+1)', (C+6p^2+8p-1, C+6p^2+8p, ..., C+6p^2+11p-3)'')$
...
$((A+6p-2);(B+6p^2+7p, B+6p^2+7p-1, ..., B+6p^2+4p+1)', (C+12p^2-6p+3, C+12p^2-6p+4, ..., C+12p^2-3p+1)'')$
$((A+6p-1);(B+2p+1, B+2p+2, ..., B+4p-1, B+6p^2+3p, B+6p^2+3p+1, ..., B+6p^2+4p)', (C+12p^2-3p+2, C+12p^2-3p+3, ..., C+12p^2)'')$ },

$F_{ij}^{(3)} = \{ ((C+1)'';(A+6p^2+5p-1, A+6p^2+5p-2, ..., A+6p^2+2p+1), (B+6p, B+6p+1, ..., B+9p-1)')$
$((C+2)'';(A+6p^2+2p, A+6p^2+2p-1, ..., A+6p^2-p+2), (B+9p, B+9p+1, ..., B+12p-1)')$
...
$((C+2p)'';(A+10p-2, A+10p-3, ..., A+7p), (B+6p^2+3p, B+6p^2+3p+1, ..., B+6p^2+6p-1)')$
$((A+2p+1);(B+6p^2+6p, B+6p^2+6p+1, ..., B+6p^2+9p-2)', (C+6p^2, C+6p^2-1, ..., C+6p^2-3p+1)'')$
$((A+2p+2);(B+6p^2+9p-1, B+6p^2+9p, ..., B+6p^2+12p-3)', (C+6p^2-3p, C+6p^2-3p-1, ..., C+6p^2-6p+1)'')$
...

$((A+3p);(B+9p^2+2p+1, B+9p^2+2p+2, ..., B+9p^2+5p-1)', (C+3p^2+3p, C+3p^2+3p-1, ..., C+3p^2+1)'')$
$((A+3p+1);(B+9p^2+5p, B+9p^2+5p+1, ..., B+9p^2+8p-1)', (C+3p^2, C+3p^2-1, ..., C+3p^2-3p+2)'')$
$((A+3p+2);(B+9p^2+8p, B+9p^2+8p+1, ..., B+9p^2+11p-1)', (C+3p^2-3p+1, C+3p^2-3p, ..., C+3p^2-6p+3)'')$
...
$((A+4p-1);(B+12p^2-p, B+12p^2-p+1, ..., B+12p^2+2p-1)', (C+7p-2, C+7p-3, ..., C+4p)'')$
$((B+4p)';(C+6p^2+1, C+6p^2+2, ..., C+6p^2+3p-1)'', (A+4p, A+4p+1, ..., A+7p-1))$
$((B+4p+1)';(C+12p^2-2p, C+12p^2-2p-1, ..., C+12p^2-5p+1)'', (A+6p^2+5p, A+6p^2+5p+1, ..., A+6p^2+8p-2))$
$((B+4p+2)';(C+12p^2-5p, C+12p^2-5p-1, ..., C+12p^2-8p+1)'', (A+6p^2+8p-1, A+6p^2+8p, ..., A+6p^2+11p-3))$
...
$((B+6p-2)';(C+6p^2+7p, C+6p^2+7p-1, ..., C+6p^2+4p+1)'', (A+12p^2-6p+3, A+12p^2-6p+4, ..., A+12p^2-3p+1))$
$((B+6p-1)';(C+2p+1, C+2p+2, ..., C+4p-1, C+6p^2+3p, C+6p^2+3p+1, ..., C+6p^2+4p)'', (A+12p^2-3p+2, A+12p^2-3p+3, ..., A+12p^2)) \},$

$F_{ij}^{(4)} = \{ ((A+1);(C+6p^2+5p-1, C+6p^2+5p-2, ..., C+6p^2+2p+1)'', (B+6p, B+6p+1, ..., B+9p-1)')$
$((A+2);(C+6p^2+2p, C+6p^2+2p-1, ..., C+6p^2-p+2)'', (B+9p, B+9p+1, ..., B+12p-1)')$
...
$((A+2p);(C+10p-2, C+10p-3, ..., C+7p)'', (B+6p^2+3p, B+6p^2+3p+1, ..., B+6p^2+6p-1)')$
$((C+2p+1)'';(B+6p^2+6p, B+6p^2+6p+1, ..., B+6p^2+9p-2)', (A+6p^2, A+6p^2-1, ..., A+6p^2-3p+1))$
$((C+2p+2)'';(B+6p^2+9p-1, B+6p^2+9p, ..., B+6p^2+12p-3)', (A+6p^2-3p, A+6p^2-3p-1, ..., A+6p^2-6p+1))$
...
$((C+3p)'';(B+9p^2+2p+1, B+9p^2+2p+2, ..., B+9p^2+5p-1)', (A+3p^2+3p, A+3p^2+3p-1, ..., A+3p^2+1))$
$((C+3p+1)'';(B+9p^2+5p, B+9p^2+5p+1, ..., B+9p^2+8p-1)', (A+3p^2, A+3p^2-1, ..., A+3p^2-3p+2))$
$((C+3p+2)'';(B+9p^2+8p, B+9p^2+8p+1, ..., B+9p^2+11p-1)', (A+3p^2-3p+1, A+3p^2-3p, ..., A+3p^2-6p+3))$
...
$((C+4p-1)'';(B+12p^2-p, B+12p^2-p+1, ..., B+12p^2+2p-1)', (A+7p-2, A+7p-3, ..., A+4p))$
$((B+4p)';(A+6p^2+1, A+6p^2+2, ..., A+6p^2+3p-1), (C+4p, C+4p+1, ..., C+7p-1)'')$
$((B+4p+1)';(A+12p^2-2p, A+12p^2-2p-1, ..., A+12p^2-5p+1), (C+6p^2+5p, C+6p^2+5p+1, ..., C+6p^2+8p-2)'')$
$((B+4p+2)';(A+12p^2-5p, A+12p^2-5p-1, ..., A+12p^2-8p+1), (C+6p^2+8p-1, C+6p^2+8p, ..., C+6p^2+11p-3)'')$
...
$((B+6p-2)';(A+6p^2+7p, A+6p^2+7p-1, ..., A+6p^2+4p+1), (C+12p^2-6p+3, C+12p^2-6p+4, ..., C+12p^2-3p+1)'')$
$((B+6p-1)';(A+2p+1, A+2p+2, ..., A+4p-1, A+6p^2+3p, A+6p^2+3p+1, ..., A+6p^2+4p).$
$(C+12p^2-3p+2, C+12p^2-3p+3, ..., C+12p^2)'') \},$

$F_{ij}^{(5)} = \{ ((B+1)';(A+6p^2+5p-1, A+6p^2+5p-2, ..., A+6p^2+2p+1), (C+6p, C+6p+1, ..., C+9p-1)'')$
$((B+2)';(A+6p^2+2p, A+6p^2+2p-1, ..., A+6p^2-p+2), (C+9p, C+9p+1, ..., C+12p-1)'')$
...
$((B+2p)';(A+10p-2, A+10p-3, ..., A+7p), (C+6p^2+3p, C+6p^2+3p+1, ..., C+6p^2+6p-1)'')$
$((A+2p+1);(C+6p^2+6p, C+6p^2+6p+1, ..., C+6p^2+9p-2)''. (B+6p^2, B+6p^2-1, ..., B+6p^2-3p+1)')$
$((A+2p+2);(C+6p^2+9p-1, C+6p^2+9p, ..., C+6p^2+12p-3)'', (B+6p^2-3p, B+6p^2-3p-1, ..., B+6p^2-6p+1)')$
...
$((A+3p);(C+9p^2+2p+1, C+9p^2+2p+2, ..., C+9p^2+5p-1)'', (B+3p^2+3p, B+3p^2+3p-$

$1, ..., B + 3p^2 + 1)'$)
$((A+3p+1);(C+9p^2+5p, C+9p^2+5p+1, ..., C+9p^2+8p-1)'', (B+3p^2, B+3p^2-1, ..., B+3p^2-3p+2)')$
$((A + 3p + 2);(C + 9p^2 + 8p, C + 9p^2 + 8p + 1, ..., C + 9p^2 + 11p - 1)'', (B + 3p^2 - 3p + 1, B + 3p^2 - 3p, ..., B + 3p^2 - 6p + 3)')$
...
$((A+4p-1);(C+12p^2-p, C+12p^2-p+1, ..., C+12p^2+2p-1)'', (B+7p-2, B+7p-3, ..., B+4p)')$
$((C + 4p)'';(B + 6p^2 + 1, B + 6p^2 + 2, ..., B + 6p^2 + 3p - 1)', (A + 4p, A + 4p + 1, ..., A + 7p - 1))$
$((C + 4p + 1)'';(B + 12p^2 - 2p, B + 12p^2 - 2p - 1, ..., B + 12p^2 - 5p + 1)', (A + 6p^2 + 5p, A + 6p^2 + 5p + 1, ..., A + 6p^2 + 8p - 2))$
$((C + 4p + 2)'';(B + 12p^2 - 5p, B + 12p^2 - 5p - 1, ..., B + 12p^2 - 8p + 1)', (A + 6p^2 + 8p - 1, A + 6p^2 + 8p, ..., A + 6p^2 + 11p - 3))$
...
$((C + 6p - 2)'';(B + 6p^2 + 7p, B + 6p^2 + 7p - 1, ..., B + 6p^2 + 4p + 1)', (A + 12p^2 - 6p + 3, A + 12p^2 - 6p + 4, ..., A + 12p^2 - 3p + 1))$
$((C + 6p - 1)'';(B + 2p + 1, B + 2p + 2, ..., B + 4p - 1, B + 6p^2 + 3p, B + 6p^2 + 3p + 1, ..., B + 6p^2 + 4p)', (A + 12p^2 - 3p + 2, A + 12p^2 - 3p + 3, ..., A + 12p^2)) \},$

$F_{ij}^{(6)} = \{ ((C+1)'';(B+6p^2+5p-1, B+6p^2+5p-2, ..., B+6p^2+2p+1)', (A+6p, A+6p+1, ..., A+9p-1))$
$((C + 2)'';(B + 6p^2 + 2p, B + 6p^2 + 2p - 1, ..., B + 6p^2 - p + 2)', (A + 9p, A + 9p + 1, ..., A + 12p - 1))$
...
$((C + 2p)'';(B + 10p - 2, B + 10p - 3, ..., B + 7p)', (A + 6p^2 + 3p, A + 6p^2 + 3p + 1, ..., A + 6p^2 + 6p - 1))$
$((B+2p+1)';(A+6p^2+6p, A+6p^2+6p+1, ..., A+6p^2+9p-2), (C+6p^2, C+6p^2-1, ..., C+6p^2-3p+1)'')$
$((B + 2p + 2)';(A + 6p^2 + 9p - 1, A + 6p^2 + 9p, ..., A + 6p^2 + 12p - 3), (C + 6p^2 - 3p, C + 6p^2 - 3p - 1, ..., C + 6p^2 - 6p + 1)'')$
...
$((B + 3p)';(A + 9p^2 + 2p + 1, A + 9p^2 + 2p + 2, ..., A + 9p^2 + 5p - 1), (C + 3p^2 + 3p, C + 3p^2 + 3p - 1, ..., C + 3p^2 + 1)'')$
$((B+3p+1)';(A+9p^2+5p, A+9p^2+5p+1, ..., A+9p^2+8p-1), (C+3p^2, C+3p^2-1, ..., C+3p^2-3p+2)'')$
$((B + 3p + 2)';(A + 9p^2 + 8p, A + 9p^2 + 8p + 1, ..., A + 9p^2 + 11p - 1), (C + 3p^2 - 3p + 1, C + 3p^2 - 3p, ..., C + 3p^2 - 6p + 3)'')$
...
$((B+4p-1)';(A+12p^2-p, A+12p^2-p+1, ..., A+12p^2+2p-1), (C+7p-2, C+7p-3, ..., C+4p)'')$
$((A + 4p);(C + 6p^2 + 1, C + 6p^2 + 2, ..., C + 6p^2 + 3p - 1)'', (B + 4p, B + 4p + 1, ..., B + 7p - 1)')$
$((A + 4p + 1);(C + 12p^2 - 2p, C + 12p^2 - 2p - 1, ..., C + 12p^2 - 5p + 1)'', (B + 6p^2 + 5p, B + 6p^2 + 5p + 1, ..., B + 6p^2 + 8p - 2)')$
$((A + 4p + 2);(C + 12p^2 - 5p, C + 12p^2 - 5p - 1, ..., C + 12p^2 - 8p + 1)'', (B + 6p^2 + 8p - 1, B + 6p^2 + 8p, ..., B + 6p^2 + 11p - 3)')$
...
$((A + 6p - 2);(C + 6p^2 + 7p, C + 6p^2 + 7p - 1, ..., C + 6p^2 + 4p + 1)'', (B + 12p^2 - 6p + 3, B + 12p^2 - 6p + 4, ..., B + 12p^2 - 3p + 1)')$
$((A+6p-1);(C+2p+1, C+2p+2, ..., C+4p-1, C+6p^2+3p, C+6p^2+3p+1, ..., C+6p^2+4p)'', (B + 12p^2 - 3p + 2, B + 12p^2 - 3p + 3, ..., B + 12p^2)') \},$

where $A = (i-1)(6p-1)$, $B = (j-1)(6p-1)$, $C = (i+j-2)(6p-1)$, and the additions are taken modulo N with residues $1, 2, ..., N$.

Then we claim that they comprise an $\tilde{S}_k$ - factorization of $K^*_{N,N,N}$.

We can see that each of them is an $\tilde{S}_k$ - factor, because it spans all vertices of $K^*_{N,N,N}$. We show that they are arc-disjoint.

Suppose that they are not arc-disjoint. In the followings, we consider $A = (i-1)(6p-1)$, $B = (j-1)(6p-1)$, $C = (i+j-2)(6p-1)$, $D = (h-1)(6p-1)$, $E = (l-1)(6p-1)$, $F = (h+l-2)(6p-1)$, $1 \le i, j, h, l \le 2p$. Note that A, B, C, D, E, F, N are integral multiples of $6p-1$.

Let (X, Y') be an arc joining from V_1 to V_2 and let x be the residue of X modulo $6p-1$. Then the arc (X, Y') can appear only in the x-th components of $F_{ij}^{(1)}$ and $F_{hl}^{(4)}$, $F_{ij}^{(3)}$ and $F_{hl}^{(5)}$, $F_{ij}^{(2)}$ and $F_{hl}^{(6)}$

according as $1 \le x \le 2p$, $2p+1 \le x \le 4p-1$, $4p \le x \le 6p-1$, respectively.
First, we assume that the common arc joining from V_1 to V_2 appears in x-th ($1 \le x \le 2p$) component $((A+x);(B+6p^2+5p-(x-1)(3p-1)-1, B+6p^2+5p-(x-1)(3p-1)-2, ..., B+6p^2+5p-(x-1)(3p-1)-(3p-1))', (C+6p-1+(x-1)3p+1, C+6p-1+(x-1)3p+2, ..., C+6p-1+(x-1)3p+3p)'')$ of $F_{ij}^{(1)}$ and x-th component $((D+x);(F+6p^2+5p-(x-1)(3p-1)-1, F+6p^2+5p-(x-1)(3p-1)\quad 2, ..., F+6p^2+5p\ -(x-1)(3p-1)-(3p-1))'', (E+6p-1+(x-1)3p+1, E+6p-1+(x-1)3p+2, ..., E+6p-1+(x-1)3p+3p)')$ of $F_{hl}^{(4)}$.
Say $((A+x),(B+6p^2+5p-(x-1)(3p-1)-y)') = ((D+x),(E+6p-1+(x-1)3p+z)')$, where $1 \le y \le 3p-1$ and $1 \le z \le 3p$.
Then $A+x \equiv D+x \pmod N$ and $B+6p^2+5p-(x-1)(3p-1)-y \equiv E+6p-1+(x-1)3p+z \pmod N$. We have $y+z-1 \equiv 0 \pmod{6p-1}$. This is impossible, because $1 \le y+z-1 \le 6p-2$.
Second,we assume that the common arc joining from V_1 to V_2 appears in $(2p+x)$-th ($1 \le x \le p$) component $((A+2p+x);(B+6p^2+6p-1+(x-1)(3p-1)+1, B+6p^2+6p-1+(x-1)(3p-1)+2, ..., B+6p^2+6p-1+(x-1)(3p-1)+(3p-1))', (C+6p^2+1-(x-1)3p-1, C+6p^2+1-(x-1)3p-2, ..., C+6p^2+1-(x-1)3p-3p)'')$ of $F_{ij}^{(3)}$ and $(2p+x)$-th component $((D+2p+x);(F+6p^2+6p-1+(x-1)(3p-1)+1, F+6p^2+6p-1+(x-1)(3p-1)+2, ..., F+6p^2+6p-1+(x-1)(3p-1)+(3p-1))'', (E+6p^2+1-(x-1)3p-1, E+6p^2+1-(x-1)3p-2, ..., E+6p^2+1-(x-1)3p-3p)')$ of $F_{hl}^{(5)}$.
Say $((A+2p+x),(B+6p^2+6p-1+(x-1)(3p-1)+y)') = ((D+2p+x),(E+6p^2+1-(x-1)3p-z)')$, where $1 \le y \le 3p-1$ and $1 \le z \le 3p$.
Then $A+2p+x \equiv D+2p+x \pmod N$ and $B+6p^2+6p-1+(x-1)(3p-1)+y \equiv E+6p^2+1-(x-1)3p-z \pmod N$. We have $y+z-1 \equiv 0 \pmod{6p-1}$. This is impossible, because $1 \le y+z-1 \le 6p-2$.
Third,we assume that the common arc joining from V_1 to V_2 appears in $(3p+x)$-th ($1 \le x \le p-1$) component $((A+3p+x);(B+9p^2+5p-1+(x-1)3p+1, B+9p^2+5p-1+(x-1)3p+2, ..., B+9p^2+5p-1+(x-1)3p+3p)', (C+3p^2+1-(x-1)(3p-1)-1, C+3p^2+1-(x-1)(3p-1)-2, ..., C+3p^2+1-(x-1)(3p-1)-(3p-1))'')$ of $F_{ij}^{(3)}$ and $(3p+x)$-th component $((D+3p+x);(F+9p^2+5p-1+(x-1)3p+1, F+9p^2+5p-1+(x-1)3p+2, ..., F+9p^2+5p-1+(x-1)3p+3p)'', (E+3p^2+1-(x-1)(3p-1)-1, E+3p^2+1-(x-1)(3p-1)-2, ..., E+3p^2+1-(x-1)(3p-1)-(3p-1))')$ of $F_{hl}^{(5)}$.
Say $((A+3p+x),(B+9p^2+5p-1+(x-1)3p+y)') = ((D+3p+x),(E+3p^2+1-(x-1)(3p-1)-z)')$, where $1 \le y \le 3p$ and $1 \le z \le 3p-1$.
Then $A+3p+x \equiv D+3p+x \pmod N$ and $B+9p^2+5p-1+(x-1)3p+y \equiv E+3p^2+1-(x-1)(3p-1)-z \pmod N$. We have $y+z-1 \equiv 0 \pmod{6p-1}$. This is impossible, because $1 \le y+z-1 \le 6p-2$.
Fourth,we assume that the common arc joining from V_1 to V_2 appears in $4p$-th component $((A+4p);(B+6p^2+1, B+6p^2+2, ..., B+6p^2+3p-1)', (C+4p-1+1, C+4p-1+2, ..., C+4p-1+3p)'')$ of $F_{ij}^{(2)}$ and $4p$-th component $((D+4p);(F+6p^2+1, F+6p^2+2, ..., F+6p^2+3p-1)'', (E+4p-1+1, E+4p-1+2, ..., E+4p-1+3p)')$ of $F_{hl}^{(6)}$.
Say $((A+4p),(B+6p^2+y)') = ((D+4p),(E+4p-1+z)')$, where $1 \le y \le 3p-1$ and $1 \le z \le 3p$.
Then $A+4p \equiv D+4p \pmod N$ and $B+6p^2+y \equiv E+4p-1+z \pmod N$. We have $z-y+3p-1 \equiv 0 \pmod{6p-1}$. This is impossible, because $1 \le z-y+3p-1 \le 6p-2$.
Fifth,we assume that the common arc joining from V_1 to V_2 appears in $(4p+x)$-th ($1 \le x \le 2p-2$) component $((A+4p+x);(B+12p^2-2p+1-(x-1)3p-1, B+12p^2-2p+1-(x-1)3p-2, ..., B+12p^2-2p+1-(x-1)3p-3p)', (C+6p^2+5p-1+(x-1)(3p-1)+1, C+6p^2+5p-1+(x-1)(3p-1)+2, ..., C+6p^2+5p-1+(x-1)(3p-1)+3p-1)'')$ of $F_{ij}^{(2)}$ and $(4p+x)$-th component $((D+4p+x);(F+12p^2-2p+1-(x-1)3p-1, F+12p^2\quad 2p+1-(x-1)3p-2, ..., F+12p^2\quad 2p+1-(x-1)3p-3p)'', (E+6p^2+5p-1+(x-1)(3p-1)+1, E+6p^2+5p-1+(x-1)(3p-1)+2, ..., E+6p^2+5p-1+(x-1)(3p-1)+3p-1)')$ of $F_{hl}^{(6)}$.
Say $((A+4p+x),(B+12p^2-2p+1-(x-1)3p-y)') = ((D+4p+x),(E+6p^2+5p-1+(x-1)(3p-1)+z)')$, where $1 \le y \le 3p$ and $1 \le z \le 3p-1$.
Then $A+4p+x \equiv D+4p+x \pmod N$ and $B+12p^2-2p+1-(x-1)3p-y \equiv E+6p^2+5p-1+(x-1)(3p-1)+z \pmod N$. We have $y+z-1 \equiv 0 \pmod{6p-1}$. This is impossible, because

$1 \leq y+z-1 \leq 6p-2$.
Last, we assume that the common arc joining from V_1 to V_2 appears in $(6p-1)$-th component $((A+6p-1);(B+2p+1, B+2p+2, ..., B+2p+2p-1, B+6p^2+3p-1+1, B+6p^2+3p-1+2, ..., B+6p^2+3p-1+p+1)', (C+12p^2-3p+1+1, C+12p^2-3p+1+2, ..., C+12p^2-3p+1+3p-1)'')$ of $F_{ij}^{(2)}$ and $(6p-1)$-th component $((D+6p-1);(F+2p+1, F+2p+2, ..., F+2p+2p-1, F+6p^2+3p-1+1, F+6p^2+3p-1+2, ..., F+6p^2+3p-1+p+1)'', (E+12p^2-3p+1+1, E+12p^2-3p+1+2, ..., E+12p^2-3p+1+3p-1)')$ of $F_{hl}^{(6)}$.
Say $((A+6p-1),(B+2p+y)') = ((D+6p-1),(E+12p^2-3p+1+z)')$, where $1 \leq y \leq 2p-1$ and $1 \leq z \leq 3p-1$.
Then $A+6p-1 \equiv D+6p-1 \pmod{N}$ and $B+2p+y \equiv E+12p^2-3p+1+z \pmod{N}$. We have $y-z+3p-1 \equiv 0 \pmod{6p-1}$. This is impossible, because $1 \leq y-z+3p-1 \leq 5p-3$.
Say $((A+6p-1),(B+6p^2+3p-1+y)') = ((D+6p-1),(E+12p^2-3p+1+z)')$, where $1 \leq y \leq p+1$ and $1 \leq z \leq 3p-1$.
Then $A+6p-1 \equiv D+6p-1 \pmod{N}$ and $B+6p^2+3p-1+y \equiv E+12p^2-3p+1+z \pmod{N}$. We have $y-z+5p-2 \equiv 0 \pmod{6p-1}$. This is impossible, because $2p \leq y-z+5p-2 \leq 6p-2$.
Thus, there is no common arc joining from V_1 to V_2.
Similarly, there are no common arcs joining from V_1 to V_3, from V_2 to V_1, from V_2 to V_3, from V_3 to V_1, or from V_3 to V_2.
Therefore, $24p^2$ $\tilde{S}_k$ - factors $F_{ij}^{(1)}$, $F_{ij}^{(2)}$, $F_{ij}^{(3)}$, $F_{ij}^{(4)}$, $F_{ij}^{(5)}$, $F_{ij}^{(6)}$ comprise an $\tilde{S}_k$ - factorization of $K^*_{N,N,N}$.
Applying Theorem 2, $K^*_{n,n,n}$ has an $\tilde{S}_k$ - factorization.

Main Theorem. $K^*_{n_1,n_2,n_3}$ has an $\tilde{S}_k$ - factorization if and only if (i) k is even, $k \geq 4$ and (ii) $n_1 = n_2 = n_3 \equiv 0 \pmod{k(k-1)/3}$ for $k \equiv 0 \pmod 6$ and $n_1 = n_2 = n_3 \equiv 0 \pmod{k(k-1)}$ for $k \equiv 2, 4 \pmod 6$.

References

[1] G. Chartrand and L. Lesniak, Graphs & Digraphs, 2nd ed. (Wadsworth, California, 1986).
[2] H. Enomoto, T. Miyamoto and K. Ushio, *C_k - factorization of complete bipartite graphs*, Graphs and Combinatorics, 4 (1988), pp. 111–113.
[3] F. Harary, Graph Theory (Addison - Wesley, Massachusetts, 1972).
[4] N. Martin, *Complete bipartite factorisations by complete bipartite graphs*, Discrete Math. 167/168 (1997), pp. 461–480.
[5] N. Martin, *Balanced bipartite graphs may be completely star-factored*, J. Comb. Designs 5 (1997), pp. 407–415.
[6] K. Ushio, *P_3 - factorization of complete bipartite graphs*, Discrete Math., 72 (1988), pp. 361–366.
[7] K. Ushio and R. Tsuruno, *P_3 - factorization of complete multipartite graphs*, Graphs and Combinatorics, 5 (1989), pp. 385–387.
[8] K. Ushio and R. Tsuruno, *Cyclic S_k - factorization of complete bipartite graphs*, Graph Theory, Combinatorics, Algorithms and Applications (SIAM, 1991), pp. 557–563.
[9] K. Ushio, *G - designs and related designs*, Discrete Math. 116 (1993), pp. 299–311.
[10] K. Ushio, *Star-factorization of symmetric complete bipartite digraphs*, Discrete Math. 167/168 (1997), pp. 593–596.
[11] K. Ushio, *$\vec{K}_{p,q}$ - factorization of symmetric complete bipartite digraphs*, To appear in Graph Theory, Combinatorics, Algorithms and Applications (New Issues Press, 1998), pp. 823–826.
[12] K. Ushio, *$\vec{C}_k$ - factorization of symmetric complete bipartite and tripartite digraphs*, J. Fac. Sci. Technol. Kinki Univ. 33 (1997), pp. 221–222.
[13] K. Ushio, *$\vec{S}_k$ - factorization of symmetric complete tripartite digraphs*, To appear in Discrete Math. (1998).
[14] H. Wang, *On $K_{1,k}$ - factorizations of a complete bipartite graph*, Discrete Math. 126 (1994), pp. 359–364.

Effective invariants of edge colourings

by

Yōhei YAMASAKI

Department of Mathematics, Osaka University
Toyonaka, Osaka, 560-0043 Japan

Abstract. This paper provides sufficient conditions to distinguish effectively any two members of a given small family of edge colourings up to isomorphism. As their example, we shall demonstrate the difference between the factorizations GK_{2n} and GA_{2n} of the complete graph K_{2n} for $n \geq 4$.

Introduction. Let g and h be edge colourings of graphs. Then we define the induced pattern invariant $[g : h]$ of g with respect to h as the number of restrictions of g isomorphic to h.

In the rest of this paper, g and h are specified. What we may choose as h is the edge colouring $c_{2\cdot m}$ of a cyclic graph C_{2m} with every colour appearing exactly twice on an opposite pair, where m is 2 or 3.

As g, we may choose the 1-factorization GK_{2n} or GA_{2n} of the complete graph K_{2n} for a positive integer n.

In the former case, we label all the vertices as $1-n$, $2-n$, $\cdots\cdots$, $n-1$, and ∞. Then an edge of a factor F_i $(1-n \leq i \leq n-1)$ is obtained so that the sum of the end vertices is congruent to $2i$ modulo N except for the edge between i and ∞ where N denotes $2n-1$ (see Figure 1).

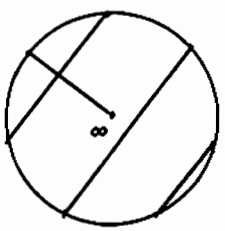


Figure 1

In the latter case, let I_n be the set of n consequent integers from $\lfloor 1-n/2 \rfloor$ to $\lfloor n/2 \rfloor$. Then vertices are chosen in $V = (0, 1) \times I_n$. We divide V into two parts V_0 and V_1, according to the first entry. We classify the factors into two types.

Suppose first that n is odd. Then a factor F_i $(i \in I_n\text{-}(0))$ of first type consists of the edges between the two parts of V such that the difference, in each, from the second entry of the vertex in V_0 to that in V_1 is congruent to i modulo n. A factor F'_i $(i \in I_n)$ of second type consists of edges among each part such that the sum of the second entry, in each, is congruent to $2i$ modulo n and, additionally, the vertical edge between $(0, i)$ and $(1, i)$ (see Figure 2-1 and 2-2).

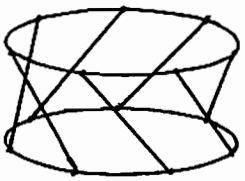


Figure 2-1

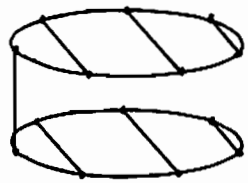


Figure 2-2

Next suppose that n is even. Then a factor F_i $(i \in I_n)$ of first type consists of the edges between the two parts of V such that the difference, in each, from the second entry of the vertex in V_0 to that in V_1 is congruent to i modulo n. A factor F'_i $(i \in I_n\text{-}(n/2))$ of second type consists of the edges among each part such that the second entries coincides with i and $n/2$, or otherwise, none of them is $n/2$ and their sum is congruent to $2i$ modulo $n\text{-}1$ (see Figure 3-1 and 3-2).

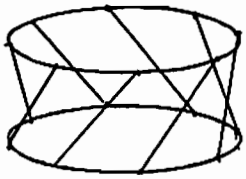


Figure 3-1

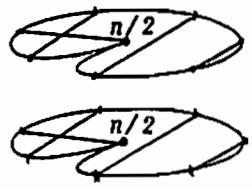


Figure 3-2

Conclusions.

Theorem. *The 1-factorizations* GK_{2n} *and* GA_{2n} *are non-isomorphic for a sufficiently large* n.

The purpose of this paper is to prove this theorem. Let a and b be positive integers. Then we define the delta function $\delta_{a,b}(n)$ as follows:

$$\delta_{a,b}(n) = \begin{cases} 1 & \text{if } n \equiv b \mod a, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 1. *We have the following equation:*

$$[GK_{2n} : C_{2\cdot 2}] = N\delta_{3,0}(N).$$

proof. Any $c_{2\cdot 2}$ pattern passes the vertex ∞ and the other vertices form a regular triangle. This fact certifies our assertion.

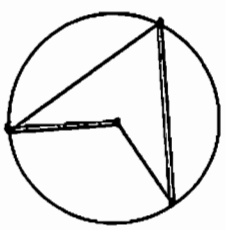
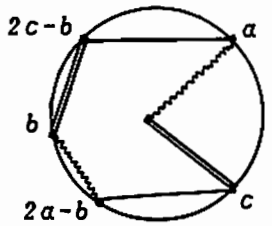


Figure 4

Lemma 2. *We have the following equation:*

$$[GK_{2n} : C_{2\cdot 3}] = N(N-1)(N-4)(N-5)/12 - N\delta_{3,0}(N)/3.$$

proof. First there is no 6-cycles passing ∞ (see Figure 5).



$2a-b+c \equiv 2c-b+a \mod n$?

Figure 5

Distinct 3 vertices can be freely chosen alternately along a 6-cycle. The differences must be equal from each of these vertices to the opposite one along this cycle (see Figure 6).

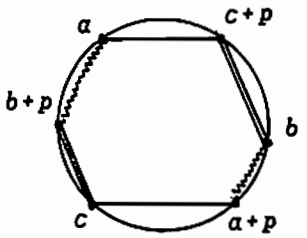


Figure 6

This value can be freely chosen out from all the possible differences among the *3* vertices modulo *N*, depending on the number of these differences. Now we have the following equation:

$$[GK_{2n} : C_{2\cdot 3}]$$
$$= N\delta_{3,0}(N)\cdot(N-3)/6 + (N(N-1) - 2N\delta_{3,0}(N))\cdot(N-5)/4$$
$$+ (N(N-1)(N-2) - 3N(N-1) + 4N\delta_{3,0}(N))\cdot(N-7)/12.$$

Thus our assertion is verified.

Lemma 3. *Let* n *be an odd number. Then we have the following equation:*

$$[GA_{2n} : C_{2\cdot 3}] = n(n-1)(n-2)(n-3)/6 + n(n-1)(n-2)(n-3)/2 + n(n-1-2\delta_{3,o}(n)) + n(n-1)(n-4)(n-5)/6 - 2n\delta_{3,o}(n)/3$$

proof. The first term indicates the numbers of patterns all of whose factors are of first type (see Figure 7).

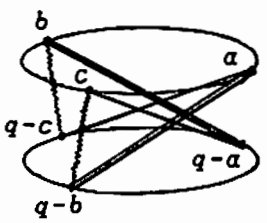


Figure 7

Next term indicates the number of patterns intersecting 2 factors of first type and 1 factor of second type, because none of such edges can be vertical (see Figure 8).

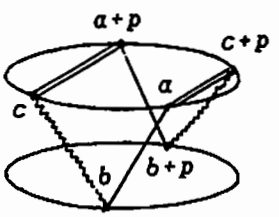
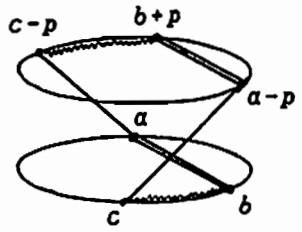


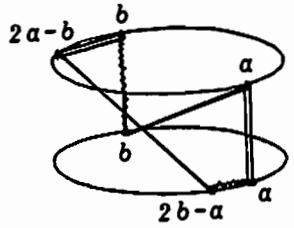
Figure 8

No patterns intersects 2 factors of second type and 1 factor of first type (see Figures 9-1 and 9-2).



$a-c+p \equiv c-a+p \mod n$?

Figure 9-1



$3a-3b \equiv a-b \mod n$?

Figure 9-2

The remaining terms indicate the numbers of patterns all of whose factors are of second type. Namely, the third indicates that with 2 vertical edges, and the rests that without vertical edges, similarly to the previous lemma (see Figure 10-1, and 10-2).

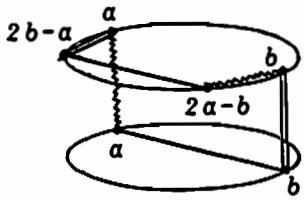


Figure 10-1

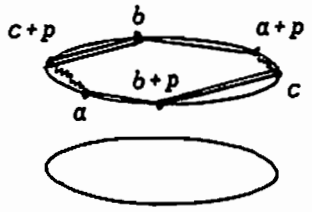


Figure 10-2

Lemma 4. *Let n be an even number exceeding 3. Then we have the following inequality:*

$$[GA_{2n} : C_{2\cdot 2}] \geq (n/2)^2.$$

proof. The right side indicates the number of patterns with both factors of first type (see Figure 11).

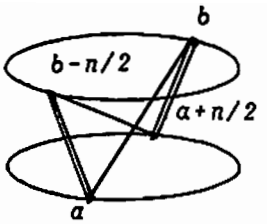


Figure 11

proof of Theorem. First suppose that n is an even number. Then by Lemma 1 and 4, we have the following inequality:

$$[GA_{2n} : C_{2\cdot 2}] - [GK_{2n} : C_{2\cdot 2}]$$
$$\geq (n/2)^2 - (2n-1)\delta_{3,2}(n).$$

Our assertion is evident since $(n/2)^2 - (2n-1) = (n/2-2)^2 - 3$ is positive for $n \geq 8$.

Suppose next that n is an odd number. Then by Lemma 2 and 3, we have the following equation:

$$[GK_{2n} : C_{2\cdot 3}] - [GA_{2n} : C_{2\cdot 3}]$$
$$= N(N-1)(N-4)(N-5)/12 - N\delta_{3,0}(N)/3$$
$$- n(n-1)(n-4)(n-5)/6 + 2n\delta_{3,0}(n)/3$$
$$- n(n-1-2\delta_{3,0}(n)) - 4n(n-1)(n-2)(n-3)/6$$

After multiplying by 6, we obtain 3 quartic polynomials with integral coefficients in n according to the classification modulo 3. Now our theorem is verified.

Binary, ternary, quaternary codes and modular forms with respect to non-compact triangle arithmetic Fuchsian groups

MASAO KOIKE

Introduction

線形コードのなかで、考えている有限体が $\mathbf{F}_2$ の場合を binary code, $\mathbf{F}_3$ の場合を ternary code, $\mathbf{F}_4$ の場合を quaternary code と呼ぶ。これらのコードと保型形式が weight enumerator（重さ枚挙多項式）を通して深くつながっていることが７０年代に Gleason,Macwilliams, Brouè-Enguehard, Maher, Sloane といった人たちによって明らかにされた。そこに現れてくるのは $SL(2,\mathbf{Z})$ とか $\Gamma_0(3)$ に関する保型形式などであった。

最近、これらの群を含むような小さなフックス群の保型形式を詳しく記述することに興味が湧いた。それは超幾何関数を通して保型形式を記述しようという試みで、従来の保型形式の研究が大通りを進むようなものとすれば、脇道をすすむようなことである。そのなかでノンコンパクト、数論的三角群とよばれる９つのフックス群に関しては、その保型形式を具体的に記述できることがわかった。この知識でもって、７０年代に行われた研究を再理解しよう、というのがこの話の主旨です。コードとの関係を調べることは坂内さんの示唆によるもので、ここで感謝の気持ちを表します。

話の構成は次のようにする。

§1 Code, weight enumerator and modular forms

§2 A road to modular forms through hypergeometric series

§3 Expression of modular forms by theta functions

1 Code, Weight enumerator and Modular forms

コードと保型形式の関係は2年前の代数学シンポジウムの報告集にのっている坂内と小関の論文と重なる部分が多いけれども、我々は、binary, ternary, quaternary codes をお互いを比較しながら議論を進めたいので、重複を恐れないで記述する。他に Sloane [13], Conway-Sloane [5] を参照。

C を binary linear code とする。自然な写像 $\rho : \mathbf{Z}^n \to \mathbf{F}_2^n$ で C を引き戻した像を $\Lambda = \frac{1}{\sqrt{2}}\rho^{-1}(C)$ と表すと、これは $\mathbf{Z}^n$ の lattice になる。そこで lattice Λ に付随するテータ関数 $\Theta_\Lambda(\tau)$ を考えれば、コードに対して保型形式が対応させられることになる：

$$\Theta_\Lambda(\tau) = \sum_{x\in\Lambda} e^{\pi i \tau\langle x,x\rangle}.$$

コードの性質として、self-dual とか doubly even とかを考えたときに、その性質が保型形式のどのような性質で記述できるかを考察することは自然である。そのとき基本になるのが $\Theta_\Lambda(\tau)$ を weight enumerator $W_C(x,y)$ と Jacobi のテータ関数を使って記述する次の公式である：

$$\Theta_\Lambda(\tau) = W_C(\theta_3(2\tau), \theta_2(2\tau)).$$

ここで $\theta_2(\tau), \theta_3(\tau)$ と書いたのは Jacobi のテータ関数で

$$\begin{aligned}\theta_3(\tau) &= 1 + 2\sum_{n=1}^{\infty} q^{1/2n^2},\\ \theta_2(\tau) &= 2\sum_{n=0}^{\infty} q^{1/2(n^2+n+1/4)}\end{aligned}$$

ここでは、我々は保型形式の習慣に従って、$q = e^{2\pi\sqrt{-1}\tau}$ と定める。有名な Gleason の定理は次のことを主張している：

定理(Gleason) C を self-dual かつ doubly even なコードとすれば、その weight enumerator $W_C(x,y)$ は次の f_1, f_2 の多項式として書ける。

$$f_1(x,y) = x^8 + 14x^4y^4 + y^8, f_2(x,y) = x^4y^4(x^4 - y^4)^4$$

さらに、$\mathbf{C}[x,y]$ の部分環で f_1, f_2 で生成される環は $\mathbf{C}[x,y]$ のある群に関する不変式環として特徴付けられることもわかっている。

ここで、保型形式との対応を書いておく：

$$\begin{aligned}f_1(\theta_3(2\tau), \theta_2(2\tau)) &= E_4(\tau),\\ f_2(\theta_3(2\tau), \theta_2(2\tau)) &= 16\Delta(\tau)\end{aligned}$$

ここで $E_4(\tau)$ はウェイト 4 の Eisenstein 級数、$\Delta(\tau)$ はウェイト 12 のカスプ形式でともに $SL(2,\mathbf{Z})$ の保型形式である。$SL(2,\mathbf{Z})$ の保型形式全体のなす環のなかで、このふたつの元で生成される環を特徴付けることはあとで整理するが、例えばウェイト 6 の Eisenstein 級数は含まれない。

binary code で self-dual かつ doubly even なものが $SL(2,\mathbf{Z})$ の保型形式と関係があることはわかったので、ternary,quaternary なコードについて同様の研究を行うのは自然のことであろう。このふたつの場合は、2 次体 $\mathbf{Q}(\sqrt{-3})$ の整数環を $\mathbf{O}$ とする。この環の素イデアルでノルムが 3、4 のもの $(\pi),(2)$ がある。それで割ってえられる剰余体がそれぞれ $\mathbf{F}_3,\mathbf{F}_4$ になる。$\mathbf{C}$ を ternary code とする。自然な写像 $\rho:\mathbf{O}^n\to\mathbf{F}_3^n$ で $\mathbf{C}$ を引き戻した像を $\Lambda=\rho^{-1}(\mathbf{C})$ と表すと、これは $\mathbf{O}^n$ の lattice になる。そこで lattice Λ に付随する次のテータ関数 $\Theta_\Lambda(\tau)$ を考えれば、コードに対して保型形式が対応させられることになる：

$$\Theta_\Lambda(\tau)=\sum_{x\in\Lambda}e^{2\pi i\tau(x,x)/3}.$$

この場合も、$\mathbf{C}$ の weight enumerator $W_\mathbf{C}(x,y)$ とテータ関数の関係が知られている。

$$\Theta_\Lambda(\tau)=W_\mathbf{C}(\psi_0(\tau),\psi_1(\tau)).$$

ここでは、代入される保型形式は次で与えられる：

$$\begin{aligned}\psi_0(\tau) &= \theta_2(2\tau)\theta_2(6\tau)+\theta_3(2\tau)\theta_3(6\tau)\\ \psi_1(\tau) &= \frac{1}{2}\left\{\psi_0(\frac{\tau}{3})-\psi_0(\tau)\right\}\end{aligned}$$

これは Ebeling の本 [6] では それぞれ θ_0,θ_1 という記号で表されている。この保型形式の weight は 1 である。

この場合も Gleason の定理にあたる次の定理が知られている。

定理 (Gleason) $\mathbf{C}$ を self-dual な ternary なコードとすれば、その weight enumerator $W_\mathbf{C}(x,y)$ は g_1,g_2 の多項式として書ける。

$$g_1(x,y)=x^4+8xy^3,g_2(x,y)=y^3(x^3-y^3)^3$$

さらに、$\mathbf{C}[x,y]$ の部分環で g_1,g_2 で生成される環は $\mathbf{C}[x,y]$ の不変式環として特徴付けられることもわかっている。

ここで、保型形式との対応を書いておく：

$$\begin{aligned}g_1(\psi_0(\tau),\psi_1(\tau)) &= E_4(\tau).\\ g_2(\psi_0(\tau),\psi_1(\tau)) &= 27\Delta(\tau)\end{aligned}$$

これはbinaryなときとそっくりである。

それではquaternaryな場合にも似たようなことがあるのだろうか?Cをquaternary codeとする。自然な写像$\rho : \mathbf{O}^n \to \mathbf{F}_4^n$でCを引き戻した像を$\Lambda = \rho^{-1}(\mathrm{C})$と表すと、これは$\mathbf{O}^n$のlatticeになる。そこでlattice Λに付随する次のテータ関数$\Theta_\Lambda(\tau)$を考えれば、コードに対して保型形式が対応させられることになる：

$$\Theta_\Lambda(\tau) = \sum_{x \in \Lambda} e^{\pi i \tau (x,x)}.$$

この場合も、Cのweight enumerator $W_\mathrm{C}(x,y)$とテータ関数の関係が知られている。

$$\Theta_\Lambda(\tau) = W_\mathrm{C}(\phi_0(\tau), \phi_1(\tau)).$$

ここでは、代入される保型形式は次で与えられる：

$$\begin{aligned} \phi_1(\tau) &= \psi_0(\tau), \\ \phi_1(\tau) &= \theta_2(2\tau)\theta_3(6\tau) + \theta_3(2\tau)\theta_2(6\tau). \end{aligned}$$

すなわち、ひとつはternaryと共通なテータ関数であるが、もうひとつは異なる。Gleasonの定理の類似は

定理 (MacWilliams,Mallows,Sloane) Cをself-dualなquaternaryなコードとすれば、そのweight enumerator $W_\mathrm{C}(x,y)$はh_1, h_2の多項式として書ける。

$$h_1(x,y) = x^2 + 3y^2, h_2(x,y) = y^2(x^2 - y^2)^2$$

さらに、$\mathrm{C}[x,y]$の部分環でg_1, g_2で生成される環は$\mathrm{C}[x,y]$のある群の不変式環として特徴付けられることもわかっている。

ところが保型形式との対応を考えると、

$$\begin{aligned} h_1(\phi_0(\tau), \phi_1(\tau)) &= E_4(\tau), \\ h_2(\phi_0(\tau), \phi_1(\tau)) &= 27\Delta(\tau) \end{aligned}$$

とはなっていない。それではこの保型形式はどこに属するのだろうか?この３つの有限体上のコードに対応するテータ関数の関係は似ている。小さなフックス群に関する保型形式をそれだけで調べるのは特別な理由がなければやってもつまらないと思う。だからほっておかれたのだが、今回別な事情から調べる理由が生まれた。その結果で７０年代のコードと保型形式の関係の研究を見直してみる。

2 A road to modular forms through Hypergeometric series

$SL_2(\mathbf{Z})$ に関する保型形式が二つの Eisenstein 級数、$E_4(\tau), E_6(\tau)$ で生成されることはよく知られている。

しかし、この Eisenstein 級数が保型関数と超幾何関数を使って次のように表されることは有名ではない。

$$E_4(\tau) = F(\frac{1}{12}, \frac{5}{12}, 1, \frac{12^3}{j(\tau)})^4,$$
$$E_6(\tau) = (1 - \frac{12^3}{j(\tau)})^{\frac{1}{2}} F(\frac{1}{12}, \frac{5}{12}, 1, \frac{12^3}{j(\tau)})^6.$$

この結果は数論で重要な合同部分群一般に拡張されることは期待できないので、面白い事実としてほっておかれた。Atkin は７６年にミシガン大学でのシンポジウムでこの事実にふれていたし、その後超特異楕円曲線との関係を研究していたようだ。その仕事に刺激されて、金子-Zagier [9] の論文が生まれる。このなかで超幾何関数と $SL(2, \mathbf{Z})$ の保型形式との面白い関係が発見された。関連する仕事として浅井-金子-二宮 [1] もある。これらの仕事を理解しようとしてこれから述べる結果が得られた。

最初に超幾何関数を定義する。α, β, γ を 0 でない複素数とする。超幾何関数 $F(\alpha, \beta, \gamma; z)$ を

$$F(\alpha, \beta, \gamma; z) = \sum_{n=0}^{\infty} \frac{(\alpha)_n (\beta)_n}{(1)_n (\gamma)_n} x^n$$

で定義する。ここで $(\alpha)_0 = 1$、正の整数 n については $(\alpha)_n = \alpha(\alpha+1)\cdots(\alpha+n-1)$ とする。

上の公式は超幾何関数の変数のところに楕円モジュラー関数 $j(\tau)$ の逆数を 12^3 倍したものを代入すれば $SL(2, \mathbf{Z})$ の保型形式である Eisenstein 級数が得られることを示している。

このフックス群、超幾何関数、保型関数という３つのつながりが大切である。前の二つについてはノンコンパクトな数論的三角群と呼ばれるものに拡張すればよいことはわかる。ノンコンパクトな数論的三角群と呼ばれる群は竹内 [16] によって９つしか存在しないことが知られている。

９つの三角群は種数が 0 のフックス群で、その保型関数体の生成元で ∞ でのみ 1 位の極をもつ関数が存在する。このなかでも６つは合同部分群であり、古くから研究がされていたが、Conway-Norton [4] による Moonshine の研究のなかでこの関数は Thompson 級数として記号が付けられている。残る３つは合同部分群ではないので、その群に関する保

型関数や保型形式の研究はあまりなされていない。しかしMoonshineの研究の発展としてreplicableな保型関数を調べたFord-Mckay-Norton [7]の結果にその群は現れているので、彼らによる群を表す記号を利用できる。

カスプ∞でのみ極をもつThompson関数は定数項を0と指定している。しかし我々の研究では、定数項を正しく求めることが重要である。当然のことながらそれらは0ではない。その保型関数はあとで具体的に与えられる。

9つの三角群の表を与える。3角群は3点での分岐指数を指定することで定まる。

1A	2,3,∞	$(\frac{1}{12}, \frac{5}{12}, 1)$	$\Gamma_0(1)$
2A	2,4,∞	$(\frac{1}{8}, \frac{3}{8}, 1)$	$\Gamma^*(2)$
2B	2,∞,∞	$(\frac{1}{4}, \frac{3}{4}, 1)$	$\Gamma_0(2)$
3A	2,6,∞	$(\frac{1}{6}, \frac{1}{3}, 1)$	$\Gamma^*(3)$
3B	3,∞,∞	$(\frac{1}{3}, \frac{2}{3}, 1)$	$\Gamma_0(3)$
4C	∞,∞,∞	$(\frac{1}{2}, \frac{1}{2}, 1)$	$\Gamma_0(4)$
2a	3,3,∞	$(\frac{1}{6}, \frac{1}{2}, 1)$	
4a	4,4,∞	$(\frac{1}{4}, \frac{1}{2}, 1)$	
6a	6,6,∞	$(\frac{1}{3}, \frac{1}{2}, 1)$	

1列はThompson関数の名前、2列は3点での分岐指数、3列は対応する超幾何関数の(α, β, γ)、4列はフックス群でよく知られている記号、が与えられている。空欄はそれらの群が保型関数の数論的な研究ではあまり扱われていない群であることを示している。

これら9つの群の互いの包含関係は竹内にある。

9つの三角群に付随する保型関数体は種数が0だから一つの関数で生成される。その生成元のなかでThompson関数と呼ばれるものは無限遠点のカスプで1位の極をもち、定

数項が 0 のものとして具体的に Conway-Norton [4],Ford-Mckay-Norton[7] で与えられている。

しかし、超幾何関数と関連させて取り扱うためには定数項を 0 とすることはむしろ不自然で、残る 2 つの分岐する点での値をこめて正しく選ばねばならない。

$1A$ の場合を考えてみる。そこでは 2 つの分岐点は $\sqrt{-1}$ と $\frac{-1+\sqrt{-3}}{2}$ で与えられ、楕円曲線の不変量で与えられる j 関数 $j(\tau)$ はそこで

$$j(\sqrt{-1}) = 12^3, j(\frac{-1+\sqrt{-3}}{2}) = 0$$

の値をとる。従って関数 $\frac{12^3}{j(\tau)}$ は基本領域と $\mathbf{P}^1$ との同型を与え、3 つの分岐点を $0, 1, \infty$ に写す写像である。

$j(\tau)$ は定数項が 744 であり、それを Thompson 関数の記号法でここでは t_{1A} と書く。

残る 8 つの三角群の場合に対しても基本領域を定め、分岐点での値を j 関数と同様の性質をみたすように定めた。次の表ではそれらの関数を、無限遠点でのフーリエ展開の係数の小さいところを具体的にあたえることで 1 意的に定めることができる。

	t_{1A}	t_{2A}	t_{2B}	t_{4C}	t_{3A}	t_{3B}
-1	1	1.	1	1	1	1
0	744	104	40	8	42	15
1	196884	4372	276	20	783	54
2	21493760	96256	-2048	0	8672	-76
3	864299970	1240002	11202	-62	65367	-243
4	20245856256	10698752	-49152	0	371520	1188
5	333202640600	74428120	184024	216	1741655	-1384
6	4252023300096	431529984	-614400	0	7161696	-2916
7	44656994071935	2206741887	1881471	-641	26567946	11934
8	401490886656000	10117578752	-5373952	0	90521472	-11580
9	3176440229784420	42616961892	14478180	1636	288078201	-21870
10	22567393309593600	166564106240	-37122048	0	864924480	79704
11	146211911499519294	611800208702	91231550	-3778	2469235686	-71022

ここでは 1 列目の n の横の行に $q^n, q = e^{2\pi\sqrt{-1}}$ のフーリエ係数が与えられている。

	t_{2a}	t_{4a}	t_{6a}
$-\frac{1}{2}$	1	1	1
0	$24\sqrt{-3}$	$16\sqrt{-1}$	$6\sqrt{-3}$
$\frac{1}{2}$	-492	-76	-33
$\frac{3}{2}$	-22590	-702	-153
$\frac{5}{2}$	-367400	-5224	-713
$\frac{7}{2}$	-3764865	-23425	-2550
$\frac{9}{2}$	-28951452	-98172	-7479
$\frac{11}{2}$	-182474434	-336450	-20314
$\frac{13}{2}$	-990473160	-1094152	-51951
$\frac{15}{2}$	-4780921725	-3188349	-122229
$\frac{17}{2}$	-20974230680	-8913752	-276656
$\frac{19}{2}$	-84963769662	-23247294	-601068

ここでは1列目の $\frac{n}{2}$ の横の行に $q^{\frac{n}{2}}$ のフーリエ係数が与えられている。

2.1 保型形式の生成する環のポアンカレ級数

Γ を9つの数論的な三角群の一つとする。kを正の偶数としてΓに関するweightがkの保型形式のなすベクトル空間を $M_k(\Gamma)$ で表す。Thompson 関数を利用して $M_k(1A)$ 等と書くことにする。

数論的三角群は分岐指数が与えられているので、それに関する保型形式の空間の次元は簡単に求められる。$d_k(\Gamma)$ を空間 $M_k(\Gamma)$ の次元として、対応する環のポアンカレ級数を

$$P_\Gamma(u) = 1 + \sum_{k>0.even} d_k(\Gamma)u^k,$$

で与えれば、それらは次のように計算される。

Γ		$P_\Gamma(u)$	
1A	2,3,∞	$\dfrac{1}{(1-u^4)(1-u^6)}$	$\Gamma_0(1)$
2A	2,4,∞	$\dfrac{1+u^6}{(1-u^4)(1-u^8)}$	$\Gamma^*(2)$
2B	2,∞,∞	$\dfrac{1}{(1-u^2)(1-u^4)}$	$\Gamma_0(2)$
3B	3,∞,∞	$\dfrac{1+u^4}{(1-u^2)(1-u^8)}$	$\Gamma_0(3)$
4C	∞,∞,∞	$\dfrac{1}{(1-u^2)(1-u^2)}$	$\Gamma_0(4)$
2a	3,3,∞	$\dfrac{1+u^6}{(1-u^4)(1-u^6)}$	
4a	4,4,∞	$\dfrac{1+2u^6+u^8}{(1-u^4)(1-u^8)}$	

Γ		$P_\Gamma(u)$	
3A	2,6,∞	$\dfrac{1+u^4+u^6+2u^8+2u^{10}+u^{12}+2u^{14}+u^{16}+u^{18}}{(1-u^{12})(1-u^{12})}$	$\Gamma^*(3)$
6a	6,6,∞	$\dfrac{1+u^4+2u^6+3u^8+4u^{10}+3u^{12}+4u^{14}+3u^{16}+2u^{18}+u^{20}}{(1-u^{12})(1-u^{12})}$	

2.2 保型形式の生成元

前の節で保型形式の生成する環のポアンカレ級数が求まったので、どの weight の保型形式を得れば、全体の保型形式が求められるかわかった。

ここでは、9つの三角群それぞれについて、生成する保型形式を超幾何関数を用いて具体的に与えていく。

その方法は1Aのときに、Eisenstein 級数が超幾何関数と Thompson 級数を用いて、次のように具体的に書けたことを利用する。

$$\begin{aligned} E_4(\tau) &= F(\frac{1}{12},\frac{5}{12},1,\frac{12^3}{j(\tau)})^4, \\ &= 1+240q+2160q^2+6720q^3+\cdots \end{aligned}$$

$$\begin{aligned} E_6(\tau) &= (1-\frac{12^3}{j(\tau)})^{\frac{1}{2}}F(\frac{1}{12},\frac{5}{12},1,\frac{12^3}{j(\tau)})^6 \\ &= 1-504q-16632q^2-122976q^3+\cdots \end{aligned}$$

さらに、この二つの式から $SL_2(\mathbb{Z})$ の weight 12 のカスプ形式　$\Delta(\tau)$ が

$$\begin{aligned} \Delta(\tau) &= \frac{E_4(\tau)^3-E_6(\tau)^2}{12^3} \\ &= \frac{1}{j(\tau)}F(\frac{1}{12},\frac{5}{12},1,\frac{12^3}{j(\tau)})^{12} \\ &= q-24q^2+252q^3+\cdots \\ &= \eta(\tau)^{24}, \end{aligned}$$

これらの保型形式が超幾何関数で書けている形と $M_k(1A)$ の次元をみれば、$E_4(\tau), E_6(\tau)$ が保型形式の空間の生成元になることが明かになる。この式のなかでは $\eta(\tau)$ を使って表示すること以外は自明である。

今までの結果から、上の等式で、9つの三角群の各々について、どの超幾何関数をとればよいか、どの Thompson 級数をとればよいかわかっている。それらを計算して保型形式の生成元を具体的に求めていく。

Case of 2A

$P_{2A}(u) = \dfrac{1+u^6}{(1-u^4)(1-u^8)}$ だから weight 4,6,8 の保型形式を探す。

$$\begin{aligned} F(\tfrac{1}{8},\tfrac{3}{8},1,\frac{256}{t_{2A}(\tau)})^4 &= 1+48q+624q^2+1344q^3+5232q^4+\cdots \\ &= \frac{1}{5}\{E_4(\tau)+4E_4(2\tau)\} \end{aligned}$$

$$\begin{aligned} (1-\frac{256}{t_{2A}(\tau)})^{\frac{1}{2}}F(\tfrac{1}{8},\tfrac{3}{8},1,\frac{256}{t_{2A}(\tau)})^6 &= 1-56q-2296q^2-13664q^3-73976q^4+\cdots \\ &= \frac{1}{9}\{E_6(\tau)+8E_6(2\tau)\} \\ \frac{1}{t_{2A}(\tau)}F(\tfrac{1}{8},\tfrac{3}{8},1,\frac{256}{t_{2A}(\tau)})^8 &= q-8q^2+12q^3+64q^4+64q^5+\cdots \\ &= \eta(2\tau)^8\eta(\tau)^8 \end{aligned}$$

この3つの式のうちで最後のものはカスプ形式である。

Case of 2B

$P_{2B}(u) = \dfrac{1}{(1-u^2)(1-u^4)}$ だから weight 2,4 の保型形式を探す。

$$\begin{aligned} F(\tfrac{1}{4},\tfrac{3}{4},1,\frac{64}{t_{2B}})^2 &= 1+24q+24q^2+96q^3+24q^4+144q^5+\cdots \\ &= 2E_2(2\tau)-E_2(\tau), \\ \frac{1}{t_{2B}}F(\tfrac{1}{4},\tfrac{3}{4},1,\frac{64}{t_{2B}})^4 &= q+8q^2+28q^3+64q^4+126q^5+\cdots \\ &= \frac{\eta(2\tau)^{16}}{\eta(\tau)^8}, \end{aligned}$$

という二つの保型形式を見つけることができる。

Case of 3B

$P_{3B}(u) = \dfrac{1+u^4}{(1-u^2)(1-u^6)}$ だから weight 2,4,6 の保型形式を探す。

$$\begin{aligned} F(\frac{1}{3},\frac{2}{3},1,\frac{27}{t_{3B}})^2 &= 1+12q+36q^2+12q^3+84q^4+72q^5+\cdots \\ &= -\frac{1}{2}\{E_2(\tau)-3E_2(3\tau)\} \end{aligned}$$

$$\begin{aligned} (\frac{1}{t_{3B}})F(\frac{1}{3},\frac{2}{3},1,\frac{27}{t_{3B}})^4 &= q+9q^2+27q^3+73q^4+126q^5+243q^6+\cdots \\ &= \frac{1}{9}\{E_6(\tau)+8E_6(2\tau)\} \\ (\frac{1}{t_{3B}})^2F(\frac{1}{3},\frac{2}{3},1,\frac{27}{t_{3B}})^6 &= q^2+6q^3+27q^4+80q^5+207q^6+\cdots \\ &= \left(\frac{\eta(3\tau)^9}{\eta(\tau)^3}\right)^2 \end{aligned}$$

Case of 4C

$P_{4C}(u) = \dfrac{1}{(1-u^2)(1-u^2)}$ だから weight 2 の保型形式を二つ探す。

$$\begin{aligned} F(\frac{1}{2},\frac{1}{2},1,\frac{16}{t_{4C}})^2 &= 1+8q+24q^2+32q^3+24q^4+48q^5+\cdots \\ &= -\frac{1}{3}\{E_2(\tau)-4E_2(4\tau)\} \end{aligned}$$

$$\begin{aligned} \frac{1}{t_{4C}}F(\frac{1}{2},\frac{1}{2},1,\frac{16}{t_{4C}})^2 &= q+4q^3+6q^5+8q^7+\cdots \\ &= \frac{\eta(4\tau)^8}{\eta(2\tau)^4} \end{aligned}$$

Case of 2a

$P_{2a}(u) = \dfrac{1+u^6}{(1-u^4)(1-u^6)}$ だから weight 4,6 の保型形式を探す。

$$\begin{aligned} \left(1-\frac{48\sqrt{-3}}{t_{2a}}\right)^{\frac{1}{3}} F(\frac{1}{6},\frac{1}{2},1,\frac{48\sqrt{-3}}{t_{2a}})^4 &= 1+240q+2160q^2+6720q^3+\cdots \\ &= E_4(\tau) \end{aligned}$$

$$F(\frac{1}{6},\frac{1}{2},1,\frac{48\sqrt{-3}}{t_{2a}})^6 = 1+24\sqrt{-3}q^{\frac{1}{2}}-504q-288\sqrt{-3}q^{\frac{3}{2}}$$
$$-16632q+1296\sqrt{-3}q^{\frac{5}{2}}+\cdots$$
$$\frac{1}{t_{2a}}F(\frac{1}{6},\frac{1}{2},1,\frac{48\sqrt{-3}}{t_{2a}})^6 = q^{\frac{1}{2}}-12q^{\frac{3}{2}}+54q^{\frac{5}{2}}-88q^{\frac{7}{2}}+\cdots$$

Case of 4a

$$P_{4a}(u)=\frac{1+2u^6+u^8}{(1-u^4)(1-u^8)}$$

$$\left(1-\frac{32\sqrt{-1}}{t_{4a}}\right)^{\frac{1}{2}}F(\frac{1}{4},\frac{1}{2},1,\frac{32\sqrt{-1}}{t_{4a}})^4 = \frac{1}{3}\{E_4(\tau)+4E_4(2\tau)\}$$

$$\left(1-\frac{32\sqrt{-1}}{t_{4a}}\right)^{\frac{1}{4}}F(\frac{1}{4},\frac{1}{2},1,\frac{32\sqrt{-1}}{t_{4a}})^6 = 1+16\sqrt{-1}q^{\frac{1}{2}}-56q+320\sqrt{-1}q^{\frac{3}{2}}$$
$$-2296q-1184\sqrt{-1}q^{\frac{5}{2}}+\cdots$$

$$\frac{1}{t_{4a}}\left(1-\frac{32\sqrt{-1}}{t_{4a}}\right)^{\frac{1}{4}}F(\frac{1}{4},\frac{1}{2},1,\frac{32\sqrt{-1}}{t_{4a}})^6 = q^{\frac{1}{2}}+20q^{\frac{3}{2}}-74q^{\frac{5}{2}}-24q^{\frac{7}{2}}+\cdots$$

$$F(\frac{1}{4},\frac{1}{2},1,\frac{32\sqrt{-1}}{t_{4a}})^8 = 1+32\sqrt{-1}q^{\frac{1}{2}}-416q-2688\sqrt{-1}q^{\frac{3}{2}}$$
$$+7648q-2624\sqrt{-1}q^{\frac{5}{2}}+\cdots$$

$$\frac{1}{t_{4a}^2}F(\frac{1}{4},\frac{1}{2},1,\frac{32\sqrt{-1}}{t_{4a}})^8 = q-8q^2+12q^3+64q^4-210q^5-96q^6+\cdots$$

ここで分母に現れる $(1-u^4)(1-u^8)$ に対応するウェイト 4,8 の保型形式はそれぞれ

$$\left(1-\frac{32\sqrt{-1}}{t_{4a}}\right)^{\frac{1}{2}}F(\frac{1}{4},\frac{1}{2},1,\frac{32\sqrt{-1}}{t_{4a}})^4,\ \frac{1}{t_{4a}^2}F(\frac{1}{4},\frac{1}{2},1,\frac{32\sqrt{-1}}{t_{4a}})^8$$

をとる。この二つの元で生成される 2 変数の環上の上に現れた残りの元たちで生成される加群が保型形式の環となる。

Case of 3A

$$P_{4a}(u) = \frac{1 + u^4 + u^6 + 2u^8 + 2u^{10} + u^{12} + 2u^{14} + u^{16} + u^{18}}{(1 - u^{12})(1 - u^{12})}$$

$$F(\frac{1}{6}, \frac{1}{3}, 1, \frac{108}{t_{3A}(\tau)})^4 = 1 + 24q + 216q^2 + 888q^3 + 1752q^4 + \cdots$$
$$= \frac{1}{10}\{E_4(\tau) + 9E_4(3\tau)\}$$

$$\left(1 - \frac{108}{t_{3A}(\tau)}\right)^{\frac{1}{2}} F(\frac{1}{6}, \frac{1}{3}, 1, \frac{108}{t_{3A}(\tau)})^6 = 1 - 18q - 594q^2 - 4878q^3 - 19026q^4 - \cdots$$
$$= \frac{1}{28}\{E_6(\tau) + 27E_6(3\tau)\}$$

$$F(\frac{1}{6}, \frac{1}{3}, 1, \frac{108}{t_{3A}(\tau)})^8 = 1 + 48q + 1008q^2 + 12144q^3 + 92784q^4 + \cdots$$

$$\frac{1}{t_{3A}} F(\frac{1}{6}, \frac{1}{3}, 1, \frac{108}{t_{3A}(\tau)})^8 = q + 6q^2 - 27q^3 - 92q^4 + 390q^5 + \cdots$$

$$\left(1 - \frac{108}{t_{3A}(\tau)}\right)^{\frac{1}{2}} F(\frac{1}{6}, \frac{1}{3}, 1, \frac{108}{t_{3A}(\tau)})^{10} = 1 + 6q - 810q^2 - 22134q^3 - 278634q^4 - \cdots$$

$$\left(1 - \frac{108}{t_{3A}(\tau)}\right)^{\frac{1}{2}} \frac{1}{t_{3A}} F(\frac{1}{6}, \frac{1}{3}, 1, \frac{108}{t_{3A}(\tau)})^{10} = q - 36q^2 - 81q^3 + 784q^4 - 1314q^5 + \cdots$$

$$F(\frac{1}{6}, \frac{1}{3}, 1, \frac{108}{t_{3A}(\tau)})^{12} = 1 + 72q + 2376q^2 + 47592q^3 + 646344q^4 + \cdots$$

$$\frac{1}{t_{3A}} F(\frac{1}{6}, \frac{1}{3}, 1, \frac{108}{t_{3A}(\tau)})^{12} = q + 30q^2 + 333q^3 + 1444q^4 - 570q^5 + \cdots$$

$$\frac{1}{t_{3A}^2} F(\frac{1}{6}, \frac{1}{3}, 1, \frac{108}{t_{3A}(\tau)})^{12} = q^2 - 12q^3 + 54q^4 - 100q^5 + 45q^6 + \cdots$$

$$\left(1 - \frac{108}{t_{3A}(\tau)}\right)^{\frac{1}{2}} F(\frac{1}{6}, \frac{1}{3}, 1, \frac{108}{t_{3A}(\tau)})^{14} = 1 + 30q - 450q^2 - 39390q^3 - 977730q^4 - \cdots$$

$$\left(1 - \frac{108}{t_{3A}(\tau)}\right)^{\frac{1}{2}} \frac{1}{t_{3A}} F(\frac{1}{6}, \frac{1}{3}, 1, \frac{108}{t_{3A}(\tau)})^{14} = q - 12q^2 - 729q^3 - 8048q^4 - 30210q^5 + \cdots$$

$$\frac{1}{t_{3A}}F(\frac{1}{6},\frac{1}{3},1,\frac{108}{t_{3A}(\tau)})^{16} = q+54q^2+1269q^3+16804q^4+134406q^5+\cdots$$

$$\left(1-\frac{108}{t_{3A}(\tau)}\right)^{\frac{1}{2}}\frac{1}{t_{3A}}F(\frac{1}{6},\frac{1}{3},1,\frac{108}{t_{3A}(\tau)})^{18} = q+12q^2-801q^3-27248q^4-389730q^5+\cdots$$

ここで分母に現れる $(1-u^{12})^2$ に対応するウェイト 12 の保型形式は

$$F(\frac{1}{6},\frac{1}{3},1,\frac{108}{t_{3A}(\tau)})^{12},\frac{1}{t_{3A}^2}F(\frac{1}{6},\frac{1}{3},1,\frac{108}{t_{3A}(\tau)})^{12}$$

をとる。この二つの元で生成される 2 変数の環上の上に現れた残りの元たちで生成される加群が保型形式の環となる。

$6a$ に関する保型形式を超幾何関数で記述するのは長くなるので、この報告では省略させていただく。

3 テータ関数による保型形式の表現

コード理論の示すところは保型形式を二つのテータ関数の多項式として表示することが有力な研究手段であることを教えてくれる。二つのテータ関数の選び方も有限体 $\mathbf{F}_2,\mathbf{F}_3,\mathbf{F}_4$ に応じて 3 種類あることがわかっている。しかし、どんなフックス群に関する保型形式がこれらのテータ関数で表現すると面白いのかはわかっていない。

前の節で我々は 9 つの三角群に関する保型形式が具体的に表せることを示した。これらの保型形式が上の 3 種類のテータ関数で表せるという保証はないのだが、実際に計算をしてみると意外にもきれいな関係が見出せる。最初にわかったことの概略を述べる。

1. binary code から得られるテータ関数の組 $\theta_3(\tau),\theta_2(\tau)$ は 6 つの三角群 $1.4, 2.4, 2B, 4C, 2a, 4a$ の保型形式を表すことができる。
2. ternary code から得られるテータ関数の組 $\psi_0(\tau),\psi_1(\tau)$ は三角群 $3.4, 3B$ の保型形式を表すことができる。
3. quaternary code から得られるテータ関数の組 $\phi_0(\tau),\phi_1(\tau)$ は三角群 $3.4, 6a$ の保型形式を表すのに利用できる。この場合は上の二つの場合よりも複雑な様子をしている。

関連する仕事にふれておく。J.M. Borwein-P.B. Borwein [3] でも保型関数や保型形式がテータ関数を用いて表現されている。かれらの興味は算術幾何平均をきれいに説明する

テータ関数の関係式と超幾何関数で表示される保型形式との関連が知られている $4C$ の場合の拡張を探すことにある。その類似を $3B.2B$ で探すことに成功している。その結果は前の節で求めた保型形式の超幾何関数による表示を一部含んでいる。すなわち前の節で具体的に与えられた保型関数が Borwein たちによるテータ関数の商の形をしていることにもなっている。すなわち、

$$\frac{16}{t_{4C}} = \left\{\frac{\theta_2(2\tau)^2}{\theta_3(2\tau)^2}\right\}^2$$

$$\frac{64}{t_{2B}} = \left\{\frac{2\theta_2(2\tau)^2\theta_3(2\tau)^2}{\theta_3(2\tau)^4+\theta_2(2\tau)^4}\right\}^2$$

$$\frac{27}{t_{3B}} = \left\{\frac{\frac{1}{2}\left\{L(\frac{\tau}{3})-L(\tau)\right\}}{L(\tau)}\right\}^3$$

ここで $L(\tau)$ と彼らの記号で書いた関数は $\dot{\varphi}_0(\tau)=\dot{\varphi}_0(\tau)$ と同じ関数を表している。この式はこのあとで証明もされる。

3.1 binary

6つの三角群 $1A, 2A, 2B, 4C, 2a, 4a$ に関する保型形式は Jacobi のテータ関数

$$\theta_2(2\tau), \theta_3(2\tau)$$

を用いて $C[\theta_2(2\tau), \theta_3(2\tau)]$ の元として具体的に書くことができる。ただし多項式のべき指数に4の倍数ではない偶数が $2a, 4a$ では現れる。さらにこれらの場合は多項式の係数として虚二次体の数も現れる。これらの場合は今までに例がないようなので、より詳しく記述する。

Case of 1A

$$\begin{aligned} E_4(\tau) &= F(\frac{1}{12}, \frac{5}{12}, 1, \frac{12^3}{j(\tau)})^4 \\ &= \theta_2(2\tau)^8 + 14\theta_2(2\tau)^4\theta_3(2\tau)^4 + \theta_3(2\tau)^8 \end{aligned}$$

$$
\begin{aligned}
E_6(\tau) &= (1-\frac{12^3}{j(\tau)})^{\frac{1}{2}} F(\frac{1}{12},\frac{5}{12};1,\frac{12^3}{j(\tau)})^6 \\
&= \theta_2(2\tau)^{12} - 33\theta_2(2\tau)^8\theta_3(2\tau)^4 - 33\theta_2(2\tau)^4\theta_3(2\tau)^8 + \theta_3(2\tau)^{12},
\end{aligned}
$$

これはよく知られた結果である。

Case of 2A

$$
\begin{aligned}
F(\frac{1}{8},\frac{3}{8};1,\frac{256}{t_{2A}})^4 &= \frac{1}{5}\left\{E_4(\tau)+4E_4(2\tau)\right\} \\
&= \theta_2(2\tau)^8 + 2\theta_2(2\tau)^4\theta_3(2\tau)^4 + \theta_3(2\tau)^8
\end{aligned}
$$

$$
\begin{aligned}
(1-\frac{256}{t_{2A}})^{\frac{1}{2}} F(\frac{1}{8},\frac{3}{8};1,\frac{256}{t_{2A}})^6 &= \frac{1}{9}\left\{E_6(\tau)+8E_6(2\tau)\right\} \\
&= \theta_2(2\tau)^{12} - 5\theta_2(2\tau)^8\theta_3(2\tau)^4 - 5\theta_2(2\tau)^4\theta_3(2\tau)^8 + \theta_3(2\tau)^{12}
\end{aligned}
$$

$$
\begin{aligned}
\frac{1}{t_{2A}} F(\frac{1}{8},\frac{3}{8};1,\frac{256}{t_{2A}})^8 &= \eta(2\tau)^8\eta(\tau)^8 \\
&= \frac{1}{2^4}\theta_2(2\tau)^4\theta_3(2\tau)^4\left\{\theta_2(2\tau)^4 - \theta_3(2\tau)^4\right\}^2
\end{aligned}
$$

この結果は知られていない。

よって、保型関数は次ぎの表示式をもつ：

$$
t_{2A} = 2^4\frac{(\theta_2(2\tau)^8 + 2\theta_2(2\tau)^4\theta_3(2\tau)^4 + \theta_3(2\tau)^8)^2}{\theta_2(2\tau)^4\theta_3(2\tau)^4\left\{\theta_2(2\tau)^4 - \theta_3(2\tau)^4\right\}^2}
$$

Case of 2B

$$
\begin{aligned}
F(\frac{1}{4},\frac{3}{4};1,\frac{64}{t_{2B}})^2 &= 2E_2(2\tau) - E_2(\tau), \\
&= \theta_2(2\tau)^4 + \theta_3(2\tau)^4
\end{aligned}
$$

$$
\begin{aligned}
\frac{1}{t_{2B}} F(\frac{1}{4},\frac{3}{4};1,\frac{64}{t_{2B}})^4 &= \frac{\eta(2\tau)^{16}}{\eta(\tau)^8} \\
&= \frac{1}{2^4}\theta_2(2\tau)^4\theta_3(2\tau)^4
\end{aligned}
$$

したがって、保型関数のテータ関数による表示式：

$$t_{2B} = 2^4 \frac{(\theta_2(2\tau)^4 + \theta_3(2\tau)^4)^2}{\theta_2(2\tau)^4\theta_3(2\tau)^4}$$

も得られる。これが最初に引用したBorweinたちの結果と同じことになる。

この結果はよく知られている。[3].

Case of 4C

$$\begin{aligned} F(\frac{1}{2},\frac{1}{2},1,\frac{16}{t_{4C}})^2 &= -\frac{1}{3}\{E_2(\tau) - 4E_2(4\tau)\} \\ &= \theta_3(2\tau)^4 \end{aligned}$$

$$\begin{aligned} \frac{1}{t_{4C}}F(\frac{1}{2},\frac{1}{2},1,\frac{16}{t_{4C}})^2 &= \frac{\eta(4\tau)^8}{\eta(2\tau)^4} \\ &= \frac{1}{2^4}\theta_2(2\tau)^4 \end{aligned}$$

$$t_{4C} = 2^4 \frac{\theta_3(2\tau)^4}{\theta_2(2\tau)^4}$$

これもよく知られている。

Case of 2a

保型関数 t_{2a} に対して、$T_{2a} = t_{2a} - 24\sqrt{-3}$ とおけば、

$$j - 1728 = T_{2a}^2$$

と書ける。したがって

$$T_{2a} = \frac{4(\theta_2(2\tau)^{12} - 33\theta_2(2\tau)^8\theta_3(2\tau)^4 - 33\theta_2(2\tau)^4\theta_3(2\tau)^8 + \theta_3(2\tau)^{12})}{\theta_2(2\tau)^2\theta_3(2\tau)^2(\theta_2(2\tau)^4 - \theta_3(2\tau)^4)^2}$$

したがって

$$t_{2a} = \frac{4(\theta_2(2\tau)^4 + 2\sqrt{-3}\theta_2(2\tau)^2\theta_3(2\tau)^2 + \theta_3(2\tau)^4)^3}{\theta_2(2\tau)^2\theta_3(2\tau)^2(\theta_2(2\tau)^4 - \theta_3(2\tau)^4)^2}$$

が成り立つ。さらに

$$1-\frac{48\sqrt{-3}}{t_{2a}}=\frac{(\theta_2(2\tau)^4-2\sqrt{-3}\theta_2(2\tau)^2\theta_3(2\tau)^2+\theta_3(2\tau)^4)^3}{(\theta_2(2\tau)^4+2\sqrt{-3}\theta_2(2\tau)^2\theta_3(2\tau)^2+\theta_3(2\tau)^4)^3}$$

よって

$$(1-\frac{48\sqrt{-3}}{t_{2a}})^{1/3}=\frac{(\theta_2(2\tau)^4-2\sqrt{-3}\theta_2(2\tau)^2\theta_3(2\tau)^2+\theta_3(2\tau)^4)}{(\theta_2(2\tau)^4+2\sqrt{-3}\theta_2(2\tau)^2\theta_3(2\tau)^2+\theta_3(2\tau)^4)}$$

がいえる。

次の等式

$$x^8+14x^4y^4+y^8=(x^4+2\sqrt{-3}x^2y^2+y^4)(x^4-2\sqrt{-3}x^2y^2+y^4)$$

がある。

$$\left(1-\frac{48\sqrt{-3}}{t_{2a}}\right)^{\frac{1}{3}}F(\frac{1}{6},\frac{1}{2},1,\frac{48\sqrt{-3}}{t_{2a}})^4 = E_4(\tau)$$
$$= \theta_2(2\tau)^8+14\theta_2(2\tau)^4\theta_3(2\tau)^4+\theta_3(2\tau)^8$$

これは1Aの場合にすでに書いてある。

この式に上の式を代入すれば

$$F(\frac{1}{6},\frac{1}{2},1,\frac{48\sqrt{-3}}{t_{2a}})^4=(\theta_2(2\tau)^4+2\sqrt{-3}\theta_2(2\tau)^2\theta_3(2\tau)^2+\theta_3(2\tau)^4)^2$$

がでる。

したがって

$$F(\frac{1}{6},\frac{1}{2},1,\frac{48\sqrt{-3}}{t_{2a}})^6 = \left\{\theta_2(2\tau)^4+2\sqrt{-3}\theta_2(2\tau)^2\theta_3(2\tau)^2+\theta_3(2\tau)^4\right\}^3$$

$$\frac{1}{t_{2a}}F(\frac{1}{6},\frac{1}{2},1,\frac{48\sqrt{-3}}{t_{2a}})^6 = \frac{1}{4}\left\{\theta_2(2\tau)^{10}\theta_3(2\tau)^2-2\theta_2(2\tau)^6\theta_3(2\tau)^6+\theta_2(2\tau)^2\theta_3(2\tau)^{10}\right\}$$

が成り立つ。

Case of 4a

この場合にも上と同じように細かい計算をしておく。

保型関数 t_{4a} に対して、$T_{4a} = t_{4a} - 16\sqrt{-1}$ とおけば、

$$t_{2A} - 256 = T_{4a}^2$$

と書ける。したがって

$$T_{4a} = \frac{4(\theta_2(2\tau)^8 - 6\theta_2(2\tau)^4\theta_3(2\tau)^4 + \theta_3(2\tau)^8)}{\theta_2(2\tau)^2\theta_3(2\tau)^2(\theta_2(2\tau)^4 - \theta_3(2\tau)^4)}$$

したがって

$$t_{4a} = \frac{4(\theta_3(2\tau)^2 + \sqrt{-1}\theta_2(2\tau)^2)^4}{\theta_2(2\tau)^2\theta_3(2\tau)^2(\theta_2(2\tau)^4 - \theta_3(2\tau)^4)}$$

$$1 - \frac{32\sqrt{-1}}{t_{4a}} = \frac{4(\theta_3(2\tau)^2 - \sqrt{-1}\theta_2(2\tau)^2)^4}{4(\theta_3(2\tau)^2 + \sqrt{-1}\theta_2(2\tau)^2)^4}$$

ゆえに

$$\left(1 - \frac{32\sqrt{-1}}{t_{4a}}\right)^{1/2} = \frac{(\theta_3(2\tau)^2 - \sqrt{-1}\theta_2(2\tau)^2)^2}{(\theta_3(2\tau)^2 + \sqrt{-1}\theta_2(2\tau)^2)^2}$$

が成り立つ。

$$\left(1 - \frac{32\sqrt{-1}}{t_{4a}}\right)^{\frac{1}{2}} F(\frac{1}{4}, \frac{1}{2}, 1, \frac{32\sqrt{-1}}{t_{4a}})^4 = F(\frac{1}{8}, \frac{3}{8}, 1, \frac{256}{t_{2A}})^4$$
$$= \theta_2(2\tau)^8 + 2\theta_2(2\tau)^4\theta_3(2\tau)^4 + \theta_3(2\tau)^8$$

これは2Aのときと同じである。

この式に上で得られた式を代入すれば、

$$F(\frac{1}{4}, \frac{1}{2}, 1, \frac{32\sqrt{-1}}{t_{4a}})^4 = (\theta_3(2\tau)^2 + \sqrt{-1}\theta_2(2\tau)^2)^4$$

が得られる。

$$\frac{1}{t_{4a}}\left(1 - \frac{32\sqrt{-1}}{t_{4a}}\right)^{\frac{1}{4}} F(\frac{1}{4}, \frac{1}{2}, 1, \frac{32\sqrt{-1}}{t_{4a}})^6 = \frac{1}{2}\left\{\theta_3(2\tau)^{10}\theta_2(2\tau)^2 - \theta_3(2\tau)^2\theta_2(2\tau)^{10}\right\}$$

$$\frac{1}{t_{4a}}\left(1 - \frac{16\sqrt{-1}}{t_{4a}}\right) F(\frac{1}{4}, \frac{1}{2}, 1, \frac{32\sqrt{-1}}{t_{4a}})^8 = q^{\frac{1}{2}} - 84q^{\frac{3}{2}} - 82q^{\frac{5}{2}} - 456q^{\frac{7}{2}} + 4869q^{\frac{9}{2}}$$

$$= \frac{1}{4}\theta_3(2\tau)^{14}\theta_2(2\tau)^2 - \frac{7}{4}\theta_3(2\tau)^{10}\theta_2(2\tau)^6 + \frac{7}{4}\theta_3(2\tau)^6\theta_2(2\tau)^{10} - \frac{1}{4}\theta_3(2\tau)^2\theta_2(2\tau)^{14}$$

3.2 ternary

三角群 $3A, 3B$ に関する保型形式は、ternary code から得られる次の二組のテータ関数が利用できる。

$$\begin{aligned}\psi_0(\tau) &= \theta_2(2\tau)\theta_2(6\tau) + \theta_3(2\tau)\theta_3(6\tau),\\ \psi_1(\tau) &= \frac{1}{2}\left(\psi_0(\frac{\tau}{3}) - \psi_0(\tau)\right).\end{aligned}$$

Case of 3B

超幾何関数で表される保型形式とテータ関数との関係式は：

$$\begin{aligned}F(\frac{1}{3},\frac{2}{3},1,\frac{27}{t_{3B}}) &= \psi_0(\tau)\\ \frac{1}{t_{3B}}F(\frac{1}{3},\frac{2}{3},1,\frac{27}{t_{3B}})^3 &= \left\{\frac{\psi_1(\tau)}{3}\right\}^3\end{aligned}$$

この式は奇数 weight の保型形式までもふくめたテータ関数との関係を示している。我々は weight が偶数の保型形式を考えているのでこれから得られる次の関係式が必要になる：

$$F(\frac{1}{3},\frac{2}{3},1,\frac{27}{t_{3B}})^2 = \psi_0(\tau)^2$$

$$\frac{27}{t_{3B}}F(\frac{1}{3},\frac{2}{3},1,\frac{27}{t_{3B}})^4 = \psi_0(\tau)\psi_1(\tau)^3$$

$$\frac{729}{t_{3B}^2}F(\frac{1}{3},\frac{2}{3},1,\frac{27}{t_{3B}})^6 = \psi_1(\tau)^6$$

このように、$3B$ に関する保型形式は具体的に書けている。この結果は Maher [12] によってすでに知られていた。超幾何関数で書かれる部分が新しい。この結果から $3A$ に関する保型形式は上の部分集合なので同様に $C[\psi_0(\tau), \psi_1(\tau)]$ の元として書くことができることはわかる。しかし、次の節でわかるように $3A$ に関する保型形式は ternary code と関係があると同時に quaternary code とも関係がある。そのことを見るためには具体的に表すことが必要になる。しかしかなりのページを使ってしまったので次の節で結果を述べるだけにする。

3.3 quaternary

quaternary code の研究から得られた次のテータ関数の組はどんな保型形式を記述するのに利用できるのだろうか？

$$\begin{aligned}\phi_0(\tau) &= \theta_2(2\tau)\theta_2(6\tau)+\theta_3(2\tau)\theta_3(6\tau),\\ \phi_1(\tau) &= \theta_2(2\tau)\theta_3(6\tau)+\theta_3(2\tau)\theta_2(6\tau).\end{aligned}$$

残っているのは $6a$ に関する保型形式である。理由はまだよくわからないがこれが必要になる。

MacWilliams-Mallows-Sloane の定理で、 C を self-dual な quaternary なコードとすれば、その weight enumerator $W_C(x,y)$ は

$$h_1(x,y)=x^2+3y^2, h_2(x,y)=y^2(x^2-y^2)^2$$

の多項式として書ける。

この多項式に $\phi_0(2\tau),\phi_1(2\tau)$ を代入すれば正しい式は次のようになる。

$$\begin{aligned}h_1(\phi_0(2\tau),\phi_1(2\tau)) &= \phi_0(\tau)^2,\\ h_2(\phi_0(2\tau),\phi_1(2\tau)) &= F(\frac{1}{3},\frac{2}{3},1;\frac{27}{t_{3B}})^6(\frac{1}{t_{3B}}-\frac{27}{t_{3B}^2})\end{aligned}$$

すなわちこれらの式は ternary code に現れるテータ関数と quaternary code のテータ関数とを結びつける式になっている。すなわち

$$\begin{aligned}\phi_0(2\tau)^2+3\phi_1(2\tau)^2 &= \phi_0(\tau)^2=\psi_0(\tau)^2,\\ \phi_1(2\tau)^2(\phi_0(2\tau)^2-\phi_1(2\tau)^2)^2 &= \frac{1}{27}\psi_1(\tau)^3(\psi_0(\tau)^3-\psi_1(\tau)^3)\end{aligned}$$

この式から 3.A に関する保型形式を具体的に書いておけば次の定理が得られる：

定理 $S=\mathrm{C}[\phi_0(2\tau),\phi_1(2\tau)]$ とおく。k を自然数とすれば

$$M_{4k}(3.A)\subset S$$

$$M_{4k+2}(3.A)\subset \phi_0(\tau)S$$

が成り立つ。

ここで $\phi_0(\tau)^2\in S$ が成り立つことが効いている。さらに $6a$ に関する保型形式についても次の定理が成り立つ。これがいえれば上の定理はいらないのだが、発見した順序でかいておく。

定理 $S = \mathbf{C}[\phi_0(2\tau), \phi_1(2\tau)]$ とおく。k を自然数とすれば

$$M_{4k}(6a) \subset S$$

$$M_{4k+2}(6a) \subset \phi_0(\tau)S$$

が成り立つ。

上の定理で保型形式を表す多項式がどのような形をしているかはわかっていすのだが長くなったので次の機会にまわす。それは、Sに作用する有限群の不変式と関連させて調べるので、この報告はここでやめにしておく。

参考文献

[1] T. Asai, M. Kaneko and Ninomiya, Zeros of certain modular functions and an application, Comment. Math. Univ. St. Pauli 46 (1997), 93–101.

[2] M. Brouè and M. Enguehard, Polynômes des poids de certain codes et fonctions theta de certain reseaux, Ann. Sci. Ecole Norm. Sup. 6 (1973), 157–181.

[3] J.M. Borwein and P.B. Borwein, A cubic counterpart of Jacobi's identity and the AGM, Trans. A. M. S. 323 (1991), 691–701.

[4] J. Conway and S. Norton, Monstrous Moonshine, Bull.London Math. Soc. 11 (1979) ,308-339.

[5] J. Conway and N.J.A. Sloane, Sphere packings, Lattices and Groups, Springer-Verlag, 1988.

[6] W. Ebeling, Lattices and Codes, Vieweg, 1994.

[7] D. Ford,J. Mckay and S. Norton, More on replicable functions Comm. Alg. 22 (1994), 5175–5193.

[8] Y. Ihara, Schwarzian equations, J. Fac. Sci. Univ. Tokyo, Sec. 1A 21-1 (1974), 97–118.

[9] M. Kaneko and D. Zagier,Supersingular j-invariants, hypergeometric series and Atkin's orthogonal polynomials, AMS ／ IP Studies in Advanced Mathematics, 7 (1998), 97–126.

[10] M. Koike, A note on hypergeometric polynomoials over the finite field, Proc.Jangjunn Intern. Conf. of Math. Sciences, 1996.

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

[12] D.P. Maher, Modular forms from codes, Canada. J. Math. 32 (1980), 40–58.

[13] N. Sloane, Self-dual codes and lattices, Proc. Symp. in Pure Math. A. M. S. 34 (1979), 273–308.

[14] N. Sloane, Codes over GF(4) and complex lattices, J. Alg. 52 (1978), 168–181.

[15] P. Stiller, Classical Automorphic Forms and Hypergeometric Functions, J. Number Theory 28 (1988), 219–232.

[16] K. Takeuchi,A characterization of arithmetic Fuchsian groups, J. Math. Soc. Japan. 27 (1975), 600–612.

GRADUATE SCHOOL OF MATHEMATICS
KYUSHU UNIVERSITY
FUKUOKA, 812-8581
JAPAN

E-mail address: koike@math.kyushu-u.ac.jp

On harmonic weight enumerators of binary codes

Christine Bachoc

August 4, 1998

Abstract

We define some new polynomials associated to a linear binary code and a harmonic function of degree k, which generalize the usual weight enumerator of the code. When divided by $(xy)^k$, they satisfy a MacWilliams type equality. When applied to certain harmonic functions constructed from Hahn polynomials, they can compute some information on the intersection numbers of the code. We illustrate this with the extremal type II codes of length 32.

1 Introduction

As pointed out by several authors, many analogies can be found between the theory of lattices in euclidean space and the theory of codes. For example, the notion of weight enumerator corresponds in the setting of lattices to the theta series, and the MacWilliams formula, relating the weight enumerators of a code and its dual, to the Jacobi formula. While the weight enumerator is invariant under a certain matrix group, the theta series is a modular form for a certain subgroup of $Sl_2(\mathbb{Z})$.

But, while some more general theta series have been defined for long, the so-called theta series with spherical (or harmonic) coefficients, the analogous notion for codes had not been defined yet. Harmonic theta series are associated to a lattice $L \subset \mathbb{R}^n$ and to a harmonic polynomial P in n variables, and are proved by Hecke to be modular forms for a congruence group (possibly with a character). The theory of discrete harmonic functions and its connection with combinatorial designs was developed by Delsarte ([D]). We define polynomials $W_{C,f}$ associated to a binary code C and a harmonic function f of degree k and prove a MacWilliams type equality for $Z_{C,f} = (xy)^{-k} W_{C,f}$. Hence, these polynomials turn out to be invariant polynomials (possibly with a character) for the same group as the one acting on the usual weight enumerator of the code.

The most interesting application of these results is to the computation of the intersection numbers of the code, which are defined to be, for a fixed t-set T,

$$n_{w,i}(T) := \mathrm{Card}\{u \in C \mid wt(u) = w, |u \cap T| = i\}.$$

More precisely, when considering certain specific harmonic functions $H_{k,T}$ associated to T, one can derive some linear equations on the $n_{w,i}(T)$ only depending on t. In [B], this method is illustrated by the case of even formally self-dual codes of length 12, and we derive a classification of the extremal ones. We will consider here the case of extremal type II codes of length 32, and compute the general form of their coset distribution. This computation is worked out in the case of the quadratic residue code in [AP] and in the four remaining cases in [CCM].

Section 1 contains the notations and definitions. Section 2 reports on the main properties of the polynomials $W_{C,f}$ without proofs, for which the reader is sent to [B]. Section 3 is devoted to the length 32 case.

2 Definitions and notations

Let $\Omega = \{1, 2, \ldots, n\}$ be a finite set (which will be the set of coordinates of the code C) and let X be the set of its subsets, while, for all $k = 0, 1, \ldots, n$, X_k is the set of its k-subsets. We denote by $\mathbb{R}X$, $\mathbb{R}X_k$ the free real vector spaces spanned by respectively the elements of X, X_k. An element of $\mathbb{R}X_k$ is denoted by

$$f = \sum_{z \in X_k} f(z)z$$

and is identified with the real-valued function on X_k given by $z \to f(z)$. The complementary set of z is denoted by $\overline{z}$.

Such an element $f \in \mathbb{R}X_k$ can be extended to an element $\tilde{f} \in \mathbb{R}X$ by setting, for all $u \in X$,

$$\tilde{f}(u) := \sum_{\substack{z \in X_k \\ z \subset u}} f(z).$$

We may later on denote again $\tilde{f}$ by f. If an element $g \in \mathbb{R}X$ is equal to some $\tilde{f}$, for $f \in \mathbb{R}X_k$, we say that g has *degree* k. The *differentiation* γ is the operator defined by linearity from

$$\gamma(z) = \sum_{y \in X_{k-1}, y \subset z} y$$

for all $z \in X_k$ and for all $k = 0, 1, \ldots n$, and Harm_k is the kernel of γ:

$$\mathrm{Harm}_k = \mathrm{Ker}(\gamma_{|\mathbb{R}X_k}).$$

Concerning codes, we take the following notations: we freely identify words of $\mathbb{F}_2^n$ and subsets of Ω; the weight of an element $u \in \mathbb{F}_2^n$ is also the cardinality of its support and is denoted by $wt(u)$ or $|u|$. We recall some basic notions of coding theory, for which we refer to [MWS], [RS]; we only consider linear codes. The weight enumerator $W_C(x, y)$ of a binary code C is

$$W_C(x, y) := \sum_{u \in C} x^{n-wt(u)} y^{wt(u)} := \sum_{i=0}^{n} A_i x^{n-i} y^i$$

where A_i is the number of codewords of weight i and satisfies the MacWilliams identity:

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + y, x - y).$$

A type II code is a self-dual code C such that $wt(u) \equiv 0 \mod 4$ for all $u \in C$. Its weight enumerator W_C is invariant under the group $\mathcal{G}_1$ of order 192 generated by the two 2×2-matrices $T_1 := \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ and $T_2 := \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$.

One can then derive the upper bound $w(C) \leq 4([n/24] + 1)$. A code meeting this bound is said to be extremal; its weight enumerator is uniquely determined. For example, extremal type II codes of length 32 have weight 8, and their weight enumerator is equal to

$$W_C(x, y) = x^{32} + 620x^{24}y^8 + 13888x^{20}y^{12} + 36518x^{16}y^{16} + 13888x^{12}y^{20} + 620x^8y^{24} + y^{32}.$$

There are exactly five such codes ([CPS]), among which the extended quadratic residue code and a Reed-Muller code.

3 Harmonic weight enumerators

We define the harmonic weight enumerators associated to a binary linear code C and settle a MacWilliams type equality. The reader is refered to [B] for the proof.

Definition 3.1 *Let C be a binary code of length n and let $f \in Harm_k$. The harmonic weight enumerator associated to C and f is*

$$W_{C,f}(x,y) := \sum_{u \in C} \tilde{f}(u) x^{n-wt(u)} y^{wt(u)}.$$

Theorem 3.1 *Let $W_{C,f}(x,y)$ be the harmonic weight enumerator associated to the code C and the harmonic function f of degree k. Then*

$$W_{C,f}(x,y) = (xy)^k Z_{C,f}(x,y)$$

where $Z_{C,f}$ is a homogeneous polynomial of degree $n-2k$, and satisfies

$$Z_{C^\perp,f}(x,y) = (-1)^k \frac{2^{n/2}}{|C|} Z_{C,f}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right).$$

Corollary 3.1 *If C is a type II code of length n, for all $f \in Harm_k$, the polynomial $Z_{C,f}(x,y)$ belongs to the space $\mathcal{I}_{\mathcal{G}_1,\chi_k}$ of invariants for the group $\mathcal{G}_1$ and the character χ_k defined by $\chi_k(T_1) = (-1)^k$ and $\chi_k(T_2) = i^{-k}$.*

The algebra $\mathcal{I}_{\mathcal{G}_1}$ is the polynomial algebra $\mathbb{C}[P_8, P_{24}]$, where $P_8 = x^8 + 14x^4y^4 + y^8$, and $P_{24} = x^4y^4(x^4 - y^4)^4$. The spaces $\mathcal{I}_{\mathcal{G}_1,\chi_k}$ are easily seen to be ideals over the algebra $\mathcal{I}_{\mathcal{G}_1}$; they are in fact principal ideals. More precisely,

Lemma 3.1

$$\mathcal{I}_{\mathcal{G}_1,\chi_k} = \begin{cases} P_{30}\mathcal{I}_{\mathcal{G}_1} \text{ if } k \equiv 1 \mod 4, \text{ where } P_{30} = P_{12}P_{18} \\ P_{12}\mathcal{I}_{\mathcal{G}_1} \text{ if } k \equiv 2 \mod 4, \text{ where } P_{12} = x^2y^2(x^4 - y^4)^2 \\ P_{18}\mathcal{I}_{\mathcal{G}_1} \text{ if } k \equiv 3 \mod 4, \text{ where } P_{18} = xy(x^8 - y^8)(x^8 - 34x^4y^4 + y^8) \end{cases}$$

A first application of these results is to the study of the designs supported by codewords. Delsarte has given in [D] a caracterization of t-designs in terms of harmonic spaces: a set $\mathcal{B}$ of blocks is a t-design if and only if $\sum_{b \in \mathcal{B}} f(b) = 0$ for all $f \in \mathrm{Harm}_k$ and for all $k = 1 \ldots t$. Hence, the polynomials $W_{C,f}$ are a nice tool to study the designs supported by the set of words

of given weight in a code C, since, from the definition of $W_{C,f}$, they form a t-design if and only if $W_{C,f} = 0$ for all $f \in \mathrm{Harm}_k$ and for all $k = 1 \ldots t$. When combined with corollary 3.1 and lemma 3.1, one can straitforwardly recover the classical result following which the codewords of a type II extremal code form a "$t\frac{1}{2}$"-design (see [B]).

4 Example: the extremal type II codes of length 32

We show in this section how the harmonic weight enumerators can be used to compute some information on the intersection numbers of a code, illustrated by the example of the extremal type II codes of length 32.

Let T be a fixed t-set. One can attach to T some harmonic functions $H_{k,T}$ of degree k, for $1 \leq k \leq t$, the values $H_{k,T}(u)$ of which only depend on t, $|u|$ and $|u \cap T|$. They are described in [D] as the orthogonal projection of $T \in \mathbb{R}X_t$ over Harm_k. When u is itself a t-set, we have more precisely

$$H_{k,T}(u) = Q_k^t(t - |u \cap T|)$$

where the Q_k^t are Hahn polynomials ([KMcG]), and an analogous expression can be given when u has a different weight (see [B]). Let $h_{k,t}$ denote the function such that

$$H_{k,T}(u) = h_{k,t}(|u|, |u \cap T|)$$

for all t-set T and for all u.

Let us consider now the polynomial $W_{C,H_{k,T}}$. Its coefficients are linear forms in the intersection numbers $n_{w,i}(T)$:

$$W_{C,H_{k,T}}(x,y) = \sum_{u \in C} H_{k,T}(u) x^{n-wt(u)} y^{wt(u)} \tag{1}$$

$$= \sum_{w=0}^{n} \{ \sum_{i=0}^{t} h_{k,t}(w,i) n_{w,i}(T) \} x^{n-w} y^{w} \tag{2}$$

Hence, when C is a type II code, the fact that $Z_{C,H_{k,T}}(x,y)$ falls into the vector spaces described by corollary 3.1 and lemma 3.1, lead to linear equations into the coefficients of $W_{C,H_{k,T}}(x,y)$ and hence into the $n_{w,i}(T)$. We make this point more precise in the case in which we are here interested in; we assume now that C is an extremal type II code of length 32. We find

Table 1: $n_{w,i}(T)$ when $t = 4$

i	0	1	2	3	4
$w = 8$	$\lambda + 182$	$-4\lambda + 284$	$6\lambda + 126$	$-4\lambda + 28$	λ
$w = 12$	$-4\lambda + 1876$	$16\lambda + 5264$	$-24\lambda + 4872$	$16\lambda + 1680$	$-4\lambda + 196$
$w = 16$	$6\lambda + 1841$	$-24\lambda + 9128$	$36\lambda + 14580$	$-24\lambda + 9128$	$6\lambda + 1841$

that, for $k = 1, 2, 3$, the only possibility is $W_{C,H_{k,T}} = 0$, which expresses the fact that the codewords support 3-designs. In the case $k = 4$, we find that $W_{C,H_{4,T}}$ must be proportional to $(xy)^4 P_{24}$.

These properties lead to a system of linear equations, which, together with the trivial equations involving the weight enumerator of the code:

$$\sum_i n_{w,i}(T) = \text{Card}\{u \in C \mid wt(u) = w\}$$

has a unique solution when $t = 1, 2, 3$, in accordance with the 3-design property; they are also computed in [BMS], using polarisation of the Jacobi polynomial. The solutions depend affinely on one parameter when $t = 4$. In this case it is convenient to take as a parameter $\lambda = n_{8,0}(T)$ which has the following combinatorial interpretation: it is easily seen to be the number of weight 4 words in the coset $T + C$ which are different from T. It is worth noticing that, since the code has minimum distance 8, two weight 4 words in a coset are necessarily disjoint. Hence there are at most eight such words, and λ can only take the values $[0, 1, \ldots, 7]$. Moreover, the value $\lambda = 6$ is not possible because this would mean that the coset contains exactly seven words of weight 4, but, since the all-one word belongs to the code, if the coset contains seven weight 4 words, it does contain eight of them. The solutions are given in Table 1.

Moreover, the weight enumerator of the coset $T + C$ is determined by the $n_{w,i}(T)$ from the equality: $wt(T + u) = wt(u) + wt(T) - 2|u \cap T|$. We find here:

$$\begin{aligned} W_{T+C}(x, y) =& (\lambda + 1)x^{28}y^4 + (-4\lambda + 28)x^{26}y^6 + (2\lambda + 322)x^{24}y^8 \\ &+ (12\lambda + 1964)x^{22}y^{10} + (-17\lambda + 6895)x^{20}y^{12} \\ &+ (-8\lambda + 14392)x^{18}y^{14} + (28\lambda + 18332)x^{16}y^{16} + \ldots \end{aligned}$$

This expression agrees with the numerical values given in [AP] and [CCM] for the coset weight distributions of the five extremal codes. It is worth noticing that all the possible values for the parameter λ are reached. Of course, the number of time each value is taken in each code heavily depends on the code (and on its automorphism group), although the average value of λ for each code is a constant.

In the cases $t = 5, 6$, the same method leads to uniquely determined solutions, under the additional hypothesis that t is the minimum weight of the coset $T + C$, which agree with the numerical values given in [AP] and [CCM].

References

[AP] E. F. Assmus, V. Pless, *On the covering radius of extremal self-dual codes*, IEEE Trans. Inf. Th. **29** (1983) 359-363

[B] C. Bachoc, *On harmonic weight enumerators of binary codes*, preprint

[BMS] A. Bonnecaze, B. Mourrain, P. Solé, *Jacobi polynomials, type II codes, and designs*, preprint

[CCM] P. Camion, B. Courteau, A. Monpetit, *Coset weight enumerators of the extremal self-dual binary codes of length* 32, Proceedings of Eurocode 92, CISM LN **339**, Springer (1993), 17-29

[CS] J. Conway, N.J.A. Sloane, "Sphere packings, Lattices and Groups", Springer-Verlag, 1988

[CPS] J. Conway, N.J.A. Sloane, V. Pless, The binary self-dual codes of length 32: a revised enumeration, JCTA **60** (1992), 183-195

[D] P. Delsarte, *Hahn polynomials, discrete harmonics and t-designs*, SIAM J. Appl. Math. **34.1** (1978), 157-166

[Eb] W. Ebeling, "Lattices and Codes" Vieweg Editor, 1994

[KMcG] S. Karlin, J. McGregor, *The Hahn polynomials, formulas and an application*, Scripta Math. **26** (1961), 33-46

[MWS] F.J. MacWilliams, N.J.A. Sloane, "The theory of error-correcting codes", North-Holland Editor, 1977

[RS] E. Rains, N.J.A. Sloane, *Self-dual codes*, to appear in the Handbook of Coding Theory

符号理論の最近の話題

三浦晋示
ソニー（株）メディアプロセシング研究所
〒141-0001　東京都品川区北品川 6-7-35
E-mail：miura@av.crl.sony.co.jp

符号理論とは，通信システム及び記録システムの信頼性向上を目的とした誤り訂正符号の理論である．誤り訂正符号は，大きくブロック符号と畳み込み符号の２種類に分けられる．本稿ではブロック符号をとりあげ，その原理とからくりを明らかにする．ただし，通信路は記憶のないｑ元対称通信路のみを想定する．また，線形符号の最近の話題として有限体上の代数曲線論を応用した代数幾何符号がある．ここでは，その具体的構成法を紹介する．ただ残念なことに代数幾何符号の研究はいまや成熟し，それに伴い線形符号の理論研究も終焉を迎えつつある．なお，§１は無視されて§２から読み進むことも可能である．

§１　誤り訂正符号（ブロック符号）の原理とからくり

Ｆをｑ（ｑ≧２）個の元からなる有限集合とする．ｎとｋ（ｎ≧ｋ≧１）を自然数の組とする．F^kとF^nをＦ上の直積集合とする．

> Ｆ上の［ｎ，ｋ］符号（あるいは，ｑ元［ｎ，ｋ］符号）とは，
> F^kからF^nへの単射な写像をいう．ここに，ｎを符号長，ｋを情報長という．

これが，数学としての誤り訂正符号（以下，符号という）の定義の全てである．後により一般的な（より本質的な）定義を与える．以下，その目的と意味を明らかにする．

「送信者」が「受信者」に，「通信路（あるいは，記録媒体）」を介して「情報」を伝達するようすを数学的にモデル化しよう．

「情報」を，ここではＦの元の系列として捉える．
すなわち，Ｆの元を「情報」の基本単位とし，「情報」をＦの元の系列として捉えるのである．なお，状況に応じて「情報」，すなわち，Ｆの元の系列$x_1 x_2 \cdots x_k$とF^kの元（$x_1, x_2, \cdots, x_k$）とを同一視する．

「通信路」を，ある決まった時間間隔ごとにＦの元ｘを入力すると（それ以前の入力とは独立に）Ｆの元ｙがただひとつ出力されるものとする．
ただし，その条件付き確率Ｐ（ｙ｜ｘ）は，

$P(y \mid x) = 1-p$ (if $y = x$), $= p/(q-1)$ (if $y \neq x$)
に従うとする．ここに，pは「通信路」に固有の，
$0 \leqq p < 1 - 1/q$ (すなわち，$1 \geqq 1-p > p/(q-1) \geqq 0$)
なる一定の実数とする．pは「通信路」における誤りの発生確率（以下，誤り率という）である．$y \neq x$のとき誤りが発生したという．注意：入力と出力のタイミングは正確にコントロールできるとする．

「通信路」の誤り率が0ならば，「送信者」は「受信者」に「通信路」を使って「情報」（すなわち，Fの元の系列）を誤りなく正しく伝えることができる．問題は，誤り率が0とは限らない場合に起こる．このときは，「通信路」に「情報」をそのまま入力するのでは「情報」は必ずしも正しくは伝わらない．「情報」を誤りなく正しく伝えるには何らかの工夫が必要である．誤り率pが無視できない「通信路」を使って，それでいて，「情報」をより正しく伝えようというのが符号の目的である．

状況をわかりやすくするために，「通信路」は世の中にはたった一種類しか存在しないとしよう．すなわち，「通信路」の誤り率pはこれ以上の改善はできないとする．また「送信者」と「受信者」はお客様で「情報」を正しく伝えることのできる「通信路」を望まれているとする．ただし，お客様はわがままで「通信路」の使用に際してはいかなる煩わしさも嫌う．「送信者」は「情報」を「通信路」に何も考えずにただ入力したいというし，「受信者」は「通信路」から出力される「情報」が正しいか否かをいちいち判定するのはいやだという．とはいっても「通信路」は世の中にたった一種類しかなく，その誤り率pはとても無視できる値ではない．困った．どうすればよいか．

ここに，今ある「通信路」を使って，それでいて，お客様である「送信者」と「受信者」にはあたかも誤り率が無視できるほどに小さい「通信路」を使用しているかのように錯覚していただくことは，実は，可能である．ただし，遅延（入出力の時間的ずれ）の拡大と伝送速度（「通信路」の入力の時間間隔に相当）の低下は多少は我慢してもらう．それには，符号に基づく『符号器』と『復号器』と呼ばれる自動装置を開発すればよい．お客様には『符号器』と『復号器』を「通信路」の入出力の両側に取り付けた『符号器』→「通信路」→『復号器』をご所望の「通信路」にござりまするとと，提供すればよい．『符号器』と『復号器』とはいかなるものか．次にこれを説明しよう．

以下，しばらくの間「通信路」のことは忘れることにする．

ここで，自然数nを固定する．このnは，最初に掲げた符号の定義の中の符号長である．F^nを直積集合とする．

$F^n = \{(x_1, x_2, \cdots, x_n) \mid x_i \in F,\ 1 \leqq i \leqq n\}$

である．また，F^nにHamming距離d_Hを

$d_H : F^n \times F^n \to \{0, 1, \cdots, n\}$

$d_H(x, y) := \#\{i : x_i \neq y_i\}$

により定義する．ただし，

$x = (x_1, x_2, \cdots, x_n) \in F^n$，$y = (y_1, y_2, \cdots, y_n) \in F^n$である．

さて，ここで符号の定義を思い起こそう．

Fはq（q≧2）個の元からなる有限集合，nとk（n≧k≧1）は自然数の組であった．

> F^kからF^nへの単射な写像
> $\sigma : F^k \to F^n$
> を，F上の［n，k］符号という．ここに，nを符号長，kを情報長という．

これが，符号の定義の全てであった．
写像σの像をCとおく．

$C := \mathrm{Image}(\sigma) = \sigma(F^k) \subseteq F^n$

である．Cの元を符号語と呼ぶ．なお，符号の定義の本質は，実は写像σそのものというよりもその像集合としてのF^nの部分集合$C \subseteq F^n$にひそむ．あとのお楽しみ．

次に，F上の［n，k］符号$\sigma : F^k \to F^n$に付随する「符号器」と「復号器」の自動装置としての入出力を明らかにする．「符号器」と「復号器」の入出力は以下のように数学的には明確に定義される．なお，これらは「通信路」とはまったく独立に定義されることに注意せよ．

「符号器」

> 入力：$u = (u_1, u_2, \cdots, u_k) \in F^k$
> 出力：$\sigma(u) = x = (x_1, x_2, \cdots, x_n) \in C \subseteq F^n$

「(最小距離) 復号器」

> 入力：$y = (y_1, y_2, \cdots, y_n) \in F^n$
> 出力：$\{\sigma^{-1}(z) \in F^k \mid d_H(C, y) = d_H(z, y),\ z \in C\}$

ただし，$d_H(C, y) := \min\{d_H(z, y) \mid z \in C\}$ である．

次に，自然数tを指定して「(最小距離) 復号器」において$d_H(C, y) > t$のときはあえて復号をあきらめる「(t限界距離) 復号器」を定義する．

「(t限界距離) 復号器」

> 入力：$y = (y_1, y_2, \cdots, y_n) \in F^n$
> 出力：
> ・ $d_H(C, y) \leq t$のときは，
> $\{\sigma^{-1}(z) \in F^k \mid d_H(C, y) = d_H(z, y),\ z \in C\}$
> ・ $d_H(C, y) > t$のときは，
> 訂正不能を示す「信号」

以上が，「符号器」と「復号器」の入出力の数学的な定義の全てである．なお，「(0限界距離) 復号器」を特に「誤り検出器」という．

「復号器」の出力で本質をなすのは，$y \in F^n$に最も近い符号語の集合である．

$$\{z \in C \mid d_H(C, y) = d_H(z, y)\}$$

以下，これを詳しく調べよう．

ここで，F上の［n，k］符号$\sigma : F^k \to F^n$の最小距離d_{min}を，

$$d_{min} := \min \{d_H(x, z) \mid x, z \in C, x \neq z\}$$

と定義する．ただし，$C := \mathrm{Image}(\sigma) = \sigma(F^k) \subseteq F^n$である．

最小距離とは互いに異なる符号語間の距離の最小値である．

このときの符号をF上の［n，k，d_{min}］符号という．

次に，各符号語$x \in C$に対して，xを中心とする半径tの集合$D_t(x) \subseteq F^n$を次のように定義する．

$$D_t(x) := \{y \in F^n \mid d_H(x, y) \leq t\} \subseteq F^n.$$

$D_t(x) \subseteq F^n$は符号語$x \in C$の半径tの“縄張り”である．

また，最小距離の定義から任意の$x, z \in C$，$x \neq z$に関して

$$D_t(x) \cap D_t(z) = \emptyset$$

を満たすための必要十分条件は$t < d_{min}/2$（すなわち，$2t + 1 \leq d_{min}$）であることがわかる．

それ故，$d_H(C, y) \leq t < d_{min}/2$ならば，

$y \in D_t(z)$なる$z \in C$は唯一存在して，

$$\# \{z \in C \mid d_H(C, y) = d_H(z, y)\} = 1$$

である．このときは，$\{z \in C \mid d_H(C, y) = d_H(z, y)\}$を導くことは

$y \in D_t(z)$なる$z \in C$を導くことに帰着される．

これは，『（t限界距離）復号器』，$t < d_{min}/2$の出力は，訂正不能を示す「信号」か，または，F^kの元がただ一つであることを保証する．

さらに，『符号器』の出力$x \in C$と『復号器』の入力$y \in F^n$に，

$d_H(x, y) \leq t < d_{min}/2$なる関係があるときは，

$$\{z \in C \mid d_H(C, y) = d_H(z, y)\} = \{x\}$$

を満たす．これは，復号の成功を保証する．

言い換えると，yがxの半径t（$< d_{min}/2$）の“縄張り”$D_t(x)$から飛びでない限り『復号器』は復号に成功するといえる．すなわち，$t < d_{min}/2$とすると，「通信路」における誤りの発生数がt個以下である限り，いつでも『復号器』は復号に成功する．それ故，最小距離d_{min}は，符号の訂正能力をはかる上で重要なパラメータといえる．

さてここで，「通信路」を思い起こそう．まず，ここで状況を正確に把握するために「通信路」の入出力の基本単位を変えよう．見方を変えるだけである．すなわち，「通信路」の入力（すなわち，Fの元）をn個まとめてF^nの元と見なすことにより，「通信路」はF^nの元を単位に入出力されるものと解釈しなおす．このとき，「通信路」の

入力$x = (x_1, x_2, \cdots, x_n) \in F^n$と

出力$y = (y_1, y_2, \cdots, y_n) \in F^n$の

条件付き確率P（y｜x）は，仮定から，

$$P(y \mid x) = \prod_{i=1}^{n} P(y_i \mid x_i) = (1-p)^{n-d_H(x,y)} (p/(q-1))^{d_H(x,y)}$$

となる．ただし，$d_H(x, y)$ はx∈F^{n}とy∈F^{n}とのHamming距離である．
なお，$d_H(x, y)$ は「通信路」における誤りの発生数に一致することに注意せよ．
以下，エラーの発生確率pは0ではないとする．すなわち，

0＜p＜1－1／q（このとき，1＞1－p＞p／（q－1）＞0である）

とする．
このとき，P（y｜x）は$d_H(x, y)$に関して狭義の単調減少関数をなす．すなわち，y∈F^{n}に対して$d_H(x, y)$を最小にするx∈C⊆F^{n}はP（y｜x）を最大にするx∈C⊆F^{n}に一致する．

符号の導入が誤り率を小さくする“からくり”は「通信路」への入力をF^{n}の部分集合C⊆F^{n}の元に制限することにある．

ここに，「情報」がランダム系列（これは，圧縮等の技術により実現可能）であると仮定すると，『(最小距離）符号器』は実は最ゆう復号（maximum likelihood decoding），すなわち，「通信路」の出力y∈F^{n}に対して確率の最も高い「通信路」の入力x∈C⊆F^{n}を推定していることがわかる．また，「通信路」の入力xを固定したとき，「通信路」におけるエラーの発生数$d_H(x, y)$は，平均np，分散np（1－p）の2項分布に従う．nが十分大きいとき，2項分布は，平均np，分散np（1－p）の正規分布で近似できる．また，よく知られるように正規分布では，99．73％が区間$np \pm 3\sqrt{np(1-p)}$に，99．9％が区間$np \pm 3.29\sqrt{np(1-p)}$に含まれる．それ故，npに対して十分大きな自然数tを指定すると，「通信路」の入力xに関して，「通信路」における誤りの発生数$d_H(x, y)$がt個以下である確率は限りなく1に近づく．例えば，n＝10000，P＝1／100とするとnp＝100，$np+4\sqrt{np(1-p)}$＝140．・・・である．それ故，そのようなtに対して，$2t+1 \leq d_{m,n}$を満たすように符号を設計すればよい．

お客様に提供される『符号器』→「通信路」→『復号器』を念のために確認しよう．「送信者」は「情報」，すなわち，Fの元の系列$u_1u_2u_3\cdots$を逐次そのまま『符号器』に入力すればよい．『符号器』はそれを正確にk個ごとに区切りF^{k}の元$u=(u_1, u_2, \cdots, u_k) \in F^k$を単位に入力されたものとして自動処理する．『符号器』の出力$x=\sigma(u) \in C \subseteq F^n$が「通信路」に入り，「通信路」の出力y∈F^{n}が『復号器』に入る．『(t限界距離）復号器』，$t < d_{m,n}/2$からは，訂正不能を示す「信号」か，または，F^{k}の元が出力される．これらが，逐次的に自動処理される．ここに，$t < d_{m,n}/2$が十分に大きく設計されているときは，「受信者」は非常に高い確率で「送信者」の「情報」，すなわち，Fの元の系列$u_1u_2u_3\cdots$を正しく受信できる．

数学的には，符号をより一般的に定義することも可能である．こちらの定義の方が（少なくとも数学的には）本質をあからさまにする．符号を直積集合F^{n}の部分集合C⊆F^{n}として定義するのである．

F^nの部分集合
$C \subseteq F^n$
を符号という．ここに，nを符号長という．ただし，Fは有限集合である．

情報長に対応するものは実数$k = \log_q(\#C)$である．ここだけが違う．
最小距離は$d_{min} := \min |d_H(x, z)| x, z \in C, x \neq z|$である．
これも，F上の［n，k，d_{min}］符号という．
ただし，このときは，「情報」をCの元の系列として捉える．すなわち，Cの元を「情報」の基本単位とし，「情報」をCの元の系列として捉えるのである．この立場に立つならば「符号器」は必要ない．また「復号器」は，次のように定義される．

「(最小距離) 復号器」

入力：$y \in F^n$
出力：$|z \in C | d_H(C, y) = d_H(z, y)|$

「(t限界距離) 復号器」

入力：$y \in F^n$
出力：
・ $d_H(C, y) \leqq t$のときは，
$|z \in C | d_H(C, y) = d_H(z, y)|$
・ $d_H(C, y) > t$のときは，
訂正不能を示す「偽号」

［n，k，d_{min}］符号に関して，k／nを符号化率（または情報率），d_{min}／nを相対最小距離という．
符号化率は通信路に流れる情報の密度でこれは大きい方が望ましい．
また，相対最小距離は正しく訂正できる誤りの割合をあらわすのでこれも大きい方がよい．
また，符号化率と相対最小距離（厳密には（$d_{min}-1$）／2n）が同じ二つの符号は符号長の大きい方が訂正能力は高い．
これは，例えば［10，6，5］符号と［100，60，41］符号を比べればわかる．このとき，前者は10のうち2個までの誤りは訂正できる．後者は，100のうち20個までの誤りは訂正できる．これに対して［10，6，5］符号を10個ならべても100のうち20個までの誤りを訂正できるとは限らない．なぜなら誤りが全部では20個以下であっても最初の10個に3個以上の誤りがあるときは訂正できないからである．

まとめると，次のようになる．

> 二つの符号があるとき，
> 符号長，符号化率，相対最小距離
> の二つが同じなら残りの大きい方が良い符号といえる．

これで，ほぼ数学的にはすっきりした．

しかし，ことは工学である．『符号器』と『復号器』を実際に作ることができないと工学としてはまったく意味がない．

上記の意味で良い符号が見つかったとしよう．

このとき，『符号器』を如何に作るか．

写像σ：$F^k \to F^n$を装置化すればよい，なんか問題ありますか？とんでもない．

例えば，$\#F=2$，$k=1000$，$n=2000$としてみよう．

$\#F^{1000}=2^{1000}$，$\#F^{2000}=2^{2000}$である．

2^{1000}通りのものから2^{2000}通りのものへの写像を装置化する？？？

これは無理です！！！

ここに，登場するのが線形符号である．

> 何のことはないFを有限体，σを線形写像に変えるだけである．

線形写像σ：$F^k \to F^n$は，行列表現できる！

線形写像σ^{-1}：$C \to F^k$も，行列表現できる！

これで，状況ががらりと変わることはご理解いただけるであろうか．

考えてみて下さい．

> $|z \in C \mid d_H(C, y) = d_H(z, y)|$

の導出を除くと工学的な困難はすべて解消する．

§2　線形符号と代数幾何符号

Fを有限体とする．n，k（n≧k）を自然数の組とする．F上の［n，k］線形符号とはn次元線形空間F^nの次元がkの部分空間$C\subseteq F^n$をいう．nを符号長，kを情報長という．

$d_H : F^n \times F^n \to \{0, 1, \cdots, n\}$

$d_H(x, y) := \#\{i : x_i \neq y_i\}$

をHamming距離という．

$d_{min}(C) := min\{d_H(x, y) : x, y \in C, x \neq y\}$

を符号$C\subseteq F^n$の最小距離という．$d_{min}(C)$の下界を設計距離という．

任意の$x \in C$（特に，$0 \in C$）に関して，

$d_{min}(C) = d_H(C \setminus \{x\}, x) = d_H(C \setminus \{0\}, 0)$

を満たす．また，$x \in F^n$に対して，

$wt(x) := d_H(x, 0)$

を重みという．最小距離は，0でない符号語（Cの元）の最小の重みに一致する．

（ブロック型線形）符号理論の中心的課題は次の二つである．

［符号構成問題］　符号長n，符号化率k／n，相対最小距離$d_{min}(C)$／nの二つを指定したとき残りをなるべく大きくする線形符号$C\subseteq F^n$を具体的に構成する問題．□

［復号問題］　任意に指定された$z \in F^n$に対して集合

$\{x \in C : d_H(z, C) = d_H(z, x)\}$

をより少ない計算量で導く問題．あるいは限界距離復号を．□

なお，符号長，符号化率，相対最小距離が全て同じ二つの線形符号の優劣は重み分布を比較して決める．最小距離を重みとする符号語数の少ない方が勝ち．それも同じなら最小距離＋1を重みとする符号語数の少ない方が勝ち．以下，同様に比較する．これは，復号が失敗する確率に注目した比較である．

現在，これらの課題を最も一般的に捉えるものとして Goppa の代数曲線符号がある．

Fを有限体とする．また，$\mathcal{X}$をF上絶対既約な非特異（射影）代数曲線とする．$\mathcal{X}$の種数を genus($\mathcal{X}$)または簡単に g と表す．$\mathcal{X}$のF有理点の集合を$\mathcal{X}(F)$と表す．曲線$\mathcal{X}$のF上の有理関数体を Rat($\mathcal{X}$)と表す．$\mathcal{X}$のF有理的な因子のなす群，すなわち，1変数代数関数体 Rat($\mathcal{X}$)／Fの因子群を Div($\mathcal{X}$)と表す．

ここに，$\mathcal{X}$の因子$H \in Div(\mathcal{X})$に関して，

$L(H) := \{f \in Rat(\mathcal{X}) \mid (f)+H \geq 0\} \cup \{0\}$，

$\Omega(H) := \{\omega \in \Omega^1(\mathcal{X}) \mid (\omega) \geq H\} \cup \{0\}$，

$l(H) := \dim L(H)$，$i(H) := \dim \Omega(H)$とおく．ただし，$\Omega^1(\mathcal{X})$は Rat($\mathcal{X}$)の一次微分加群を表すとする．また，dim はF上のベクトル空間としての次元，(f)，(ω)はそれぞれ有理関数$f \in Rat(\mathcal{X})$，一次微分$\omega \in \Omega^1(\mathcal{X})$に付随する因子とする．

一般に，$l(H) = i(H) + \deg(H) - g + 1$ が成り立つ（Riemann-Roch Theorem）．

ここに，$P_i \in \mathcal{X}(F)$（これは1変数代数関数体 Rat($\mathcal{X}$)／Fの次数が1の座と同じ），

$i = 1,2,\cdots,n$ をF有理点とし，因子 $D \in \mathrm{Div}(\mathcal{N})$ を，$D := P_1+P_2+\cdots+P_n$ とする．
また，$G \in \mathrm{Div}(\mathcal{N})$ を $\mathrm{supp}(D) \cap \mathrm{supp}(G) = \emptyset$ なるF有理的な因子とする．ここで，線形写像 α_Ω，α_L を，

$\alpha_\Omega : \Omega(G-D) \to F^n$，$\omega \to \alpha_\Omega(\omega) = (\mathrm{res}_{P_1}\omega, \mathrm{res}_{P_2}\omega, \cdots, \mathrm{res}_{P_n}\omega)$，

$\alpha_L : L(G) \to F^n$，$f \to \alpha_L(f) = (f(P_1), f(P_2), \cdots, f(P_n))$

とおく．ただし，$\mathrm{res}_P\omega$ は留数とする．

ここに，

$C_\Omega(D,G) := \mathrm{Image}(\alpha_\Omega) \subseteq F^n$，

$C_L(D,G) := \mathrm{Image}(\alpha_L) \subseteq F^n$

をそれぞれ留数型 Goppa 符号，関数型 Goppa 符号という．
また，それらを総称して代数曲線符号という．

代数曲線符号の符号長，情報長，最小距離に関しては次の事実が成り立つ．

$1 \leqq n \leqq \#\mathcal{N}(F)$ なる任意の自然数 n に対して，
符号長を $n(C_\Omega(D,G)) = n(C_L(D,G)) = n$ と設定できる．

$C_\Omega(D,G)$ と $C_L(D,G)$ は互いに双対符号をなす（留数定理による）．
すなわち，$k(C_\Omega(D,G))+k(C_L(D,G)) = n$，$C_\Omega(D,G) = C_L(D,G)^\perp$ である．

情報長は $k(C_\Omega(D,G)) = i(G-D) - i(G)$，$k(C_L(D,G)) = l(G) - l(G-D)$ である．

最小距離 $d_{min}(C_\Omega(D,G))$，$d_{min}(C_L(D,G))$ は次式を満たす．

$$\begin{aligned} d_{min}(C_\Omega(D,G)) &= \min\{\deg(B) \mid i(G-B) - i(G) = 1,\ 0 \leqq B \leqq D,\ B \in \mathrm{Div}(\mathcal{N})\} \\ &\geqq \min\{\deg(B) \mid i(G-B) - i(G) = 1,\ B \in \mathrm{Div}(\mathcal{N})\} \\ &\geqq \deg(G) - 2g + 2, \end{aligned}$$

$$\begin{aligned} d_{min}(C_L(D,G)) &= \min\{\deg(C) \mid l(G-D+C) - l(G-D) = 1,\ 0 \leqq C \leqq D,\ C \in \mathrm{Div}(\mathcal{N})\} \\ &\geqq \min\{\deg(C) \mid l(G-D+C) - l(G-D) = 1,\ C \in \mathrm{Div}(\mathcal{N})\} \\ &\geqq n - \deg(G) \end{aligned}$$

である．

ここに，$d_C(C_\Omega(D,G)) := \deg(G) - 2g + 2$，$d_C(C_L(D,G)) := n - \deg(G)$ を，Goppa 設計距離という．特に $2g-1 \leqq \deg(G)$ ならば $l(G) = \deg(G) - g + 1$，$i(G) = 0$ である．また，$0 \leqq \deg(G) \leqq n-1$ ならば $l(G-D) = 0$，$i(G-D) = n + g - 1 - \deg(G)$ である．
特に，$G = mP$，すなわち，$\mathrm{supp}(G) = |P|$ の場合が重要である．これを一点代数曲線符号という．以上が，Goppa の代数曲線符号の概要である．

細かいことを無視すると，これは，有限体F上の種数 g（これは自然数である）の代数曲線から，次の性質を持つ［n，k，d_{min}］線形符号が作れることを主張している．

＊　n は有理点の総数を上限に自由に設定できる．

＊　k は $n \geqq k \geqq 1$ と自由に設定できる．

＊　$n - k + 1 \geqq d_{min} \geqq n - k + 1 - g$ を満たす．

これから，有限体と種数が指定されたとき有理点の総数が最も多い代数曲線が最も良い符号を作ることがわかる．

しかし抽象にすぎる．すべてを具象化しないことには工学にはならない．

L（mP）を具体化するにはL(∞P):=$\cup_{m=0}^{\infty}$L(mP)を具体化する必要がある．
それには，L(∞P)を座標環とするアフィン代数曲線の定義方程式の形を決めればよい．
これを，最後の話題とする．

以下，Fを完全体（すなわち，Fは可換体でFの任意の代数拡大は分離的）とする．なお，有限体はすべて完全体である．

F上の楕円曲線の定義方程式としてWeierstrassの標準形

$Y^2+a_1XY+a_3Y=X^3+a_2X^2+a_4X+a_6$，$a_i\in F$

が知られている[Silverman 1986]．ここに，Fの標数は任意でよい．

ここでは，このWeierstrassの標準形が以外とも思えるほど安易に，かつ自然に拡張される事実を[三浦 1997]から抜粋し紹介する．以下，Fは任意標数の完全体とする．

[定義1][三浦 1992, 三浦・神谷 1993] a，bを$2\leq a<b$なる互いに素な自然数の組とする．このとき，次の多項式$f(X,Y)\in F[X,Y]$を定義方程式とするアフィン平面曲線を$C_{a,b}$曲線と呼ぶ．

$f(X,Y):=\Sigma_{ai+bj\leq ab,\,i\geq 0,\,j\geq 0}\ \alpha_{i,j}X^iY^j$

ただし，$\alpha_{i,j}\in F$，$\alpha_{0,a}\neq 0$，$\alpha_{b,0}\neq 0$とする．□

$f(X,Y)=0$をWeierstrassの標準形に合わせるならば，

$Y^a+\Sigma_{ab>ai+bj,\,i\geq 0,\,j\geq 1}\ \alpha_{ab-ai-bj}X^iY^j=X^b+\Sigma_{ab>ai,\,i\geq 0}\ \alpha_{ab-ai}X^i$，

$\alpha_i\in F$と変形すればよい．（a，b）=（2，3）のときが，まさにWeierstrassの標準形そのものである．また，（a，b）=（2，2g+1）のときは超楕円曲線の標準形となる．一般に$C_{a,b}$曲線に関して次の事実が証明できる．

[定理2][三浦 1997] 定義1の$C_{a,b}$曲線$f(X,Y)=0$に関して次が成り立つ．

（1） $f(X,Y)\in F[X,Y]$は，F上絶対既約である．

（2） 無限遠点はただ一点P=(0:1:0)のみ（Zで斉次化）からなり，Pは高位の尖点をなす．また，点PはF上次数が1の座と見なせる．

（3） $F[x,y]:=F[X,Y]/(f(X,Y))$を座標環（整域をなす）としその商体をKとおく．このとき，$(x)_\infty=aP$，$(y)_\infty=bP$，$F[x,y]\subseteq L(\infty P)\subseteq K=F(x,y)$である．ただし，$L(\infty P):=\cup_{m=0}^{\infty}L(mP)$はPのみで極を持つF上の有理関数（Kの元）のなす環とする．

（4） $\mathrm{genus}(f(X,Y))\leq(a-1)(b-1)/2$である．

ただし，$\mathrm{genus}(f(X,Y))$は曲線$f(X,Y)=0$の種数とする．

また，$(a-1)(b-1)/2=\#|\mathbf{N}\setminus(a\mathbf{N}+b\mathbf{N})|$，Nは非負整数全体の集合である．

5） $|x^iy^j\mid 0\leq i,\ 0\leq j\leq a-1|$は座標環$F[x,y]$のF線形空間としての基底をなす．さらに，任意の自然数mに関して，$|x^iy^j\mid 0\leq i,\ 0\leq j\leq a-1,\ ai+bj\leq m|$は$F[x,y]\cap L(mP)$のF線形空間としての基底をなす．

なお，$|x^iy^j\mid 0\leq i,\ 0\leq j\leq a-1,\ ai+bj\leq ab|$は一次独立で，

$\{y^{a}\} \cup \{x^{i}y^{j} \mid 0 \leq i,\ 0 \leq j \leq a-1,\ ai+bj \leq ab\}$は一次従属である．
ここに現れる非自明な一次関係式が$f(x,y)=0$である．

（6） 次の各条件は同値である．

（a） $f(X,Y)=0$はアフィン平面曲線として非特異である．

すなわち，イデアルとして，

$(f(X,Y),\ f_X(X,Y),\ f_Y(X,Y)) = (1) = F[X,Y]$

である．ただし，$f_X(X,Y)$，$f_Y(X,Y)$は形式的な偏微分とする．

（b） $F[x,y]=L(\infty P)$．

（c） $\mathrm{genus}(f(X,Y))=(a-1)(b-1)/2$．□

[定理3][三浦 1997]

K/Fを次数が1の座Pを少なくともひとつ持つ任意の1変数代数関数体とする．
また，a，bを$2 \leq a < b$なる互いに素な自然数の組とする．
ここに，aとbが共にPの空隙値でないとすると，K/FはPを唯一の無限遠点とするアフィンモデル，

$f(X,Y) := \Sigma_{ai+bj \leq ab,\ (i,j) \neq (0,b)} \alpha_{i,j} X^{i} Y^{j},\ \alpha_{i,j} \in F,\ \alpha_{0,a} \neq 0,\ \alpha_{b,0} \neq 0$

を持つ．□

以上が，Weierstrassの標準形のアフィン平面における拡張である．ここでは（a，b），ただし，a，bは$2 \leq a < b$なる互いに素な自然数の組，に注目してWeierstrassの標準形を拡張した．

次に，これをt（≧2）次元アフィン空間上に拡張する．ここに，自然数t（≧2）を固定し，t個の正整数の組$A_t=(a_1, a_2, \cdots, a_t) \in \mathbb{Z}_+^t$に注目する．ただし，$\mathrm{g.c.d}\{a_1, a_2, \cdots, a_t\}=1$を仮定する．
ここで，$d_i := \mathrm{g.c.d}\{a_1, a_2, \cdots, a_i\}$，$1 \leq i \leq t$，$d_0 := 0$とおく．
このとき，一般に次の事実が知られている．

[補題4]

$\#|\mathbb{N} \setminus (a_1\mathbb{N} + a_2\mathbb{N} + \cdots + a_t\mathbb{N})| \leq (1 + \Sigma_{i=1}^{t}(d_{i-1}/d_i - 1)a_i)/2$

である．ここに，等号が成立するための必要十分条件は，

すべてのi，$2 \leq i \leq t$に関して，

$a_i/d_i \in (a_1/d_{i-1})\mathbb{N} + (a_2/d_{i-1})\mathbb{N} + \cdots + (a_{i-1}/d_{i-1})\mathbb{N}$

を満たすことである．なお，$t=2$のときこれはいつでも成り立つ．□

以下，補題4の等号成立条件を満たす$A_t=(a_1, a_2, \cdots, a_t) \in \mathbb{Z}_+^t$をtelescopic生成系と呼ぶ．ここで，telescopic生成系

$A_t=(a_1, a_2, \cdots, a_t) \in \mathbb{Z}_+^t$，$\mathrm{g.c.d}\{a_1, a_2, \cdots, a_t\}=1$

をひとつ固定する．なお，telescopicとは限らない一般の場合は[三浦 1997]を参照せよ．

$\mathbb{N}^t$から$\mathbb{N}$への写像Ψを，

$\Psi : \mathbf{N}' \to \mathbf{N}$, $\Psi((n_1, n_2, \cdots, n_t)) := \Sigma_{i=1}{}^{t} a_i n_i$
で定義する.
$\mathbf{N}'$のΨ-次数付単項式順序$>_\Psi$を,
$M = (m_1, m_2, \cdots, m_t)$, $N = (n_1, n_2, \cdots, n_t) \in \mathbf{N}'$
に対して,
$M >_\Psi N$を,
$\Psi(M) > \Psi(N)$, また, $\Psi(M) = \Psi(N)$のときは,
$m_1 = n_1$, $m_2 = n_2$, $\cdots$, $m_{i-1} = n_{i-1}$, $m_i < n_i$で定義する.

[定義 5][三浦 1997] $T(A_t)$, $B(A_t)$, $V(A_t) \subseteq \mathbf{N}'$を,
$T(A_t) := \{(0, n_2, \cdots, n_t) \in \{0\} \times \mathbf{N}'^{t-1} \mid 0 \leqq n_i \leqq d_{i-1} / d_i - 1,\ 2 \leqq i \leqq t\}$,
$B(A_t) := T(A_t) + \mathbf{N} \times \{0\}^{t-1}$,
$V(A_t) := \{(0,\cdots,0,d_{i-1}/d_i,0,\cdots,0) \in \{0\}^{t-1} \times \mathbf{N} \times \{0\}^{t-1} \mid 2 \leqq i \leqq t\}$
と定義する. □

$\#T(A_t) = a_1$, $\#V(A_t) = t\text{-}1$, $B(A_t) \cap V(A_t) = \varnothing$である. また, 各$M \in B(A_t)$は$\Psi(M) = \Psi(N)$を満たす$N \in \mathbf{N}'$の$\Psi$-次数付単項式順序$>_\Psi$に関する最小の元であり, Ψの$B(A_t)$への制限は$B(A_t) \subseteq \mathbf{N}'$から Image$(\Psi) = a_1\mathbf{N} + a_2\mathbf{N} + \cdots + a_t\mathbf{N} \subseteq \mathbf{N}$への全単射写像を導く. また, $V(A_t) + \mathbf{N}' = \mathbf{N}' \setminus B(A_t)$である.
ここで, X_1, X_2, $\cdots$, X_tを形式的文字とした
多項式環$F[\underline{X}] := F[X_1, X_2, \cdots, X_t]$を考える.
$N = (n_1, n_2, \cdots, n_t) \in \mathbf{N}'$に対して
$\underline{X}^N = X_1{}^{n_1} X_2{}^{n_2} \cdots X_t{}^{n_t}$とする.

[定義 6][三浦 1997] (t-1 個からなる) 各$M \in V(A_t)$に対して,
$f_M(\underline{X}) := \underline{X}^M + \Sigma_{M >_\Psi N,\ N \in B(A_t)} \alpha_N \underline{X}^N \in F[\underline{X}]$, $\alpha_N \in F$
とする. ただし, αもMに依存し, $\Sigma_{M >_\Psi N,\ N \in B(A_t)}$は$M >_\Psi N$なる$N \in B(A_t)$,
すなわち, $\Psi(M) \geqq \Psi(N)$なる$N \in B(A_t)$にわたり,
$\Psi(M) = \Psi(N)$なる$N \in B(A_t)$に関して$\alpha_N \neq 0$とする. □

あるいは, Weierstrass の標準形を意識して各$M \in V(A_t)$に対して,
$f_M(\underline{X}) := \underline{X}^M + \Sigma_{M >_\Psi N,\ N \in B(A_t)} \alpha_{\Psi(M) - \Psi(N)} \underline{X}^N \in F[\underline{X}]$, $\alpha_{\Psi(M) - \Psi(N)} \in F$
ただし, $\alpha_0 \neq 0$ (αもMに依存する) とせよ.

[定理 7][三浦 1997] 定義 6 の t-1 個からなる定義方程式$f_M(\underline{X}) \in F[\underline{X}]$, $M \in V(A_t)$に関して次が成り立つ.
(1) イデアル ($\{f_M(\underline{X}) \in F[\underline{X}] \mid M \in V(A_t)\}$) $\subseteq F[\underline{X}]$は, $F[\underline{X}]$の余次元 1 の素イデアルをなす. すなわち, 定義方程式$f_M(\underline{X}) \in F[\underline{X}]$, $M \in V(A_t)$は, F上絶対既約なアフィン代数曲線を定義する. また, これは complete intersection をなす.
(2) 無限遠点はただ一点Pのみからなり, Pは高位の尖点をなす. また, 点PはF上

次数が1の座と見なせる．

（3）　$F[\underline{x}]:=F[\underline{X}]/(|f_M(\underline{X})\in F[\underline{X}] \mid M\in V(A_t)|)$ を座標環（整域をなす）としその商体をKとおく．このとき，K／Fは full constant な1変数代数関数体をなし $(x_t)_\infty=a_t P$，$1\leqq i\leqq t$，$F[\underline{x}]\subseteq L(\infty P)\subseteq K=F(\underline{x})$ である．ただし，$L(\infty P):=\cup_{m=0}^{\infty}L(mP)$ はPのみで極を持つF上の有理関数（Kの元）のなす環とする．

（4）　$\mathrm{genus}(K/F)\leqq(1+\Sigma_{i=1}^{t}(d_{i-1}/d_i-1)a_i)/2$ である．

ただし，genus(K／F)は1変数代数関数体K／Fの種数とする．

5）　$|\underline{x}^N \mid N\in B(A_t)|$ は座標環 $F[\underline{x}]$ のF線形空間としての基底をなす．さらに，任意の自然数mに関して，$|\underline{x}^N \mid N\in B(A_t),\ \Psi(N)\leqq m|$ は $F[\underline{x}]\cap L(mP)$ のF線形空間としての基底をなす．

なお，各 $M\in V(A_t)$ に対して，$|\underline{x}^N \mid N\in B(A_t),\ \Psi(N)\leqq\Psi(M)|$ は一次独立で，$|\underline{x}^M|\cup|\underline{x}^N \mid N\in B(A_t),\ \Psi(N)\leqq\Psi(M)|$ は一次従属である．

ここに現れる非自明な一次関係式が $f_M(\underline{x})=0$ である．

（6）　次の各条件は同値である．

（a）　定義方程式 $f_M(\underline{X})\in F[\underline{X}]$，$M\in V(A_t)$ はアフィン代数曲線として非特異である．すなわち，イデアルとして，

$$(|f_M(\underline{X})\in F[\underline{X}] \mid M\in V(A_t)|\cup|f_{MX_i}(\underline{X})\in F[\underline{X}] \mid M\in V(A_t),\ 1\leqq i\leqq t|)$$
$$=(1)=F[\underline{X}]$$

である．ただし，$f_{MX_i}(\underline{X})$ は $f_M(\underline{X})$ の X_i による形式的な偏微分とする．

（b）　$F[\underline{x}]=L(\infty P)$．

（c）　$\mathrm{genus}(K/F)=(1+\Sigma_{i=1}^{t}(d_{i-1}/d_i-1)a_i)/2$．□

注意：定義方程式 $f_M(\underline{X})\in F[\underline{X}]$，$M\in V(A_t)$ は Ψ-次数付単項式順序 $>_\Psi$ に付随する Grobner basis をなす．また，その△集合は $B(A_t)$ である．□

例　$t=3$，$A_3=(4,6,5)$ とする．$d_1=4$，$d_2=2$，$d_3=1$ である．

$T(A_3)=|(0,0,0),\ (0,0,1),\ (0,1,0),\ (0,1,1)|$ である．

このときの定義方程式 $f_M(\underline{X})\in F[X,Y,Z]$，$M\in V(A_3)=|(0,2,0),\ (0,0,2)|$ は，

$$Y^2+a_0X^3+a_1YZ+a_2XY+a_3XZ+a_4X^2+a_5Y+a_7Z+a_8X+a_{12},$$
$$Z^2+b_0XY+b_1XZ+b_2X^2+b_4Y+b_5Z+b_6X+b_{10},$$

ただし，$a_0\neq 0$，$b_0\neq 0$ の二つである．

ここに，見かけ上の種数は 4 で無限遠点における見かけ上の空隙列は|1,2,3,7| である．□

[Silverman 1986]　Silverman,J. The Arithmetic of Elliptic Curves. Springer-Verlag, New York.

[三浦 1992]　三浦晋示「ある平面上の代数幾何符号」
電子通信学会論文誌　A　Vol.J75-A No.11 pp.1735-1745　1992

[三浦・神谷 1993]　S.Miura,N.Kamiya:'Geometric Goppa codes on some maximal curves and their minimum distance',in Proc.1993 IEEE Information Theory Workshop,Shizuoka Japan, June 4-8, 1993,pp.85-86.

[三浦 1997]　三浦晋示「代数幾何に基づく誤り訂正符号の研究」学位論文　東京大学

Laguerre Character Sums

斉藤 直道 (上智大学)

1 Introduction.

q を奇素数 p のベキとし、q 個の元をもつ有限体を $\mathbb{F}_q$ と書く。$\mathbb{F}_q$ の乗法群を $\mathbb{F}_q^\times$、$\mathbb{F}_q$ の乗法的(加法的) 指標の全体を $\hat{\mathbb{F}}_q^\times$ ($\hat{\mathbb{F}}_q^+$) と書く。$A, B, C, M, N, \chi \in \hat{\mathbb{F}}_q^\times$ とする。1 または ε により $\mathbb{F}_q^\times$ の単位指標を、ϕ により quadratic 指標を表すことにする。任意の $N \in \hat{\mathbb{F}}_q^\times$ に対して $N(0) = 0$ とし、$\overline{N}$ を $N\overline{N} = 1$ により定義する。$x \in \mathbb{F}_q$ に対して $\lambda_0(x) = \zeta^x := \exp\left(\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)\right)$ と定義する。$\lambda_0 \in \hat{\mathbb{F}}_q^+, \lambda_0 \neq 1$ である。$w \in \mathbb{F}_q^\times, x \in \mathbb{F}_q$ に対して ${}^w\lambda_0(x) := \lambda_0(wx)$ と定義する。${}^w\lambda_0 \in \hat{\mathbb{F}}_q^+$ である。任意の $\mu \in \hat{\mathbb{F}}_q^+ - \{1\}$ は $\mu = {}^w\lambda_0 (w \in \hat{\mathbb{F}}_q^\times)$ と書ける。以下、$\mathbb{F}_q$ の元 u 全体をわたる和を省略して $\sum_u$ と書く。同様に、乗法的指標 N 全体をわたる和を省略して $\sum_N$ と書く。

さて、整数論において重要な $\mathbb{F}_q$ 上の Gauss 和、Jacobi 和はそれぞれ、$M, N \in \hat{\mathbb{F}}_q^\times$ に対して

$$G(N) = \sum_u N(u)\zeta^u \text{ (Gauss 和)}, \quad J(M,N) = \sum_u M(u)N(1-u) \text{ (Jacobi 和)}$$

と定義される。一方、特殊関数の Gamma 関数、Beta 関数はそれぞれ、次のような積分表示式が知られている。

$$\Gamma(n) = \int_0^\infty u^n e^{-u}\frac{du}{u} \text{ (Gamma 関数)}, \quad \beta(m,n) = \int_0^1 u^m(1-u)^n\frac{du}{u(1-u)} \text{ (Beta 関数)}$$

Gauss 和は Gamma 関数の、Jacobi 和は Beta 関数の、それぞれ有限体上における類似となっている。また、Beta 関数を Gamma 関数を使って書く公式

$$\beta(m,n) = \frac{\Gamma(m)\Gamma(n)}{\Gamma(m+n)}$$

に対応して、Jacobi 和を Gauss 和を使って書く公式

$$J(M,N) = \frac{G(M)G(N)}{G(MN)} \quad \text{if } MN \neq 1$$

が知られている。

このような特殊関数と有限体上の指標和の間の類似性に着目して、Evans [1] は Hermite 和、Legendre 和、そして、Laguerre 和、をそれぞれ対応する特殊関数の積分表示式から次の様に定義した。

$$H_n(x) = \frac{1}{\Gamma(-n)}\int_0^\infty u^{-n}e^{-u^2-2xu}\frac{du}{u} \text{ (Hermite 多項式)}$$

$$H_N(x) := \frac{1}{G(\overline{N})}\sum_u \overline{N}(u)\zeta^{u^2+2xu} \text{ (Hermite 和)}$$

$$P_n(x) = \frac{1}{2\pi i}\int_C u^{-n}(1-2xu+u^2)^{-\frac{1}{2}}\frac{du}{u} \text{ (Legendre 多項式)}$$

$$P_N(x) := \frac{1}{q}\sum_u N(u)\phi(1-2xu+u^2) \quad \text{(Legendre 和)}$$

$$L_n^a(x) = \frac{1}{2\pi i}\int_C u^{-n}(1+u)^{a+n}e^{-xu}\frac{du}{u} \quad \text{(Laguerre 多項式)}$$

$$L_N^A(x) := \frac{1}{q}\sum_u \overline{N}(u)AN(1+u)\zeta^{xu} \quad \text{(Laguerre 和)}$$

Evans の論文 [1] では、これらのうち特に Hermite 和についてのみ考察し数々の公式を与えている。Greene [2] は超幾何関数に対応する指標和 (超幾何指標和) を定義し、Evans と同様の考察を行った。Sawabe [8] は Legendre 和の性質について考察し Legendre 和と超幾何指標和の関係を示した。今回、Laguerre 和についていくつかの公式が得られた。 [7] §2 ではこれらを紹介する。

Greene [3] は有限特殊線型群 $SL(2,q)$ のある表現の行列成分として超幾何指標和が現れることを示した。これと同様に Laguerre 和がある群のある表現の行列成分として現れることが分った。[7] これより、有限群の表現論の簡単な補題を利用して、Laguerre 和に関する公式をさらに 2 つ得た。§3 ではこれらについて述べる。

2 Formulas of Laguerre Character Sums.

ここでは Laguerre 和についてのいくつかの公式を紹介する。

まず、x に関する n 階微分 $\left(\frac{d}{dx}\right)^n$ の類似 D^N を $F:\mathbb{F}_q \longrightarrow \mathbb{C}$ に対して

$$D^N F(x) := \frac{1}{G(\overline{N})}\sum_u \overline{N}(u)F(x-u) \quad x\in\mathbb{F}_q$$

と定義する。[1, (2.8)] n 階微分 $\left(\frac{d}{dx}\right)^n$ を含む公式

$$L_n^a(x) = \frac{x^{-a}e^x}{n!}\left(\frac{d}{dx}\right)^n\left(x^{a+n}e^{-x}\right) \quad \textbf{Rodrigues formula [6, p.204(3)]} \quad \text{に対応して}$$

公式 1 $x\neq 0$ ならば $L_N^A(x) = \dfrac{G(\overline{N})\overline{A}(x)\zeta^{-x}}{qN(-1)}D^N\left(AN(x)\zeta^x\right)$ である。

特に $N\neq 1$ のとき $L_N^A(x) = \dfrac{\overline{A}(x)\zeta^{-x}}{G(N)}D^N\left(AN(x)\zeta^x\right)$ である。 ■

また $\dfrac{d}{dx}L_n^a(x) = -L_{n-1}^{a+1}(x)$ [6, p.203(11)] に対応して

公式 2 $D^M L_N^A(x) = M(-1)L_{NM}^{AM}(x)$ である。 ■

[1, Th.4.3] と同様に次の公式が成り立つ。

公式 3 $MN\neq 1$ ならば $D^M\left(A(x)\zeta^x L_N^A(x)\right) = \dfrac{G(\overline{N})M(-1)A\overline{M}(x)\zeta^x}{G(\overline{NM})}L_{NM}^{A\overline{M}}(x)$ である。 ■

$L_N^A(x)$ で、$N=1$ のとき、x が $-x$ のとき、$x=0$ のとき、はそれぞれ次の 3 つの公式で与えられる。

公式 4 $x\neq 0$ ならば $L_1^A(x) = -\dfrac{1}{q} + \dfrac{G(A)\overline{A}(x)\zeta^{-x}}{q}$ である。 ■

公式 5 $L_N^A(-x) = A(-1)\zeta^x L_{\overline{AN}}^{\overline{A}}(x)$ である。 ■

公式 6 $L_N^A(0) = \binom{AN}{N}$ である。ただし $\binom{A}{N} := \frac{N(-1)}{q} J(A, \overline{N})$ である。[2] ■

Laguerre 関数の generating function $\frac{1}{(1-t)^{1+a}} e^{\frac{-xt}{1-t}} = \sum_{n=0}^{\infty} L_n^a(x) t^n$ [6, p.202(4)] に対応して

公式 7 $t \neq 0, 1$ ならば $\overline{A}(1-t)\zeta^{\frac{xt}{1-t}} = \frac{q}{q-1} \sum_N L_N^A(x) N(t)$ である。 ■

$e^{-ax} = (a+1)^{-a-1} \sum_{n=0}^{\infty} \left(\frac{a}{a+1}\right)^n L_n^a(x)$ [4, p.90(4.24.3)] に対応して

公式 8 $a \neq 0, -1$ ならば $\zeta^{ax} = \frac{q}{q-1} \overline{A}(a+1) \sum_N N\left(\frac{a}{a+1}\right) L_N^A(x)$ である。 ■

Greene は confluent hypergeometric function

$$ {}_1F_1\left(\begin{matrix} a \\ b \end{matrix}\middle| x\right) = \frac{\Gamma(b)}{\Gamma(a)\Gamma(b-a)} \int_0^1 t^a (1-t)^{b-a} e^{xt} \frac{dt}{t(1-t)} \quad [6, \text{p.124(9)}] $$

に対応して、confluent hypergeometric sum を次の様に定義した。

$$ {}_1F_1\left(\begin{matrix} A \\ B \end{matrix}\middle| x\right) := \varepsilon(x) AB(-1) \sum_t A(t) B\overline{A}(1-t)\zeta^{-xt} \quad [3, (5.20)] $$

$L_n^a(x) = \frac{(1+a)_n}{n!} {}_1F_1\left(\begin{matrix} -n \\ 1+a \end{matrix}\middle| x\right)$ [6, p.200(1)] に対応して

公式 9 $x \neq 0$ ならば $L_N^A(x) = \frac{A(-1)}{q} {}_1F_1\left(\begin{matrix} \overline{N} \\ A \end{matrix}\middle| x\right)$ である。 ■

$L_n^{a+b+1}(x+y) = \sum_{m=0}^{n} L_m^a(x) L_{n-m}^b(y)$ [6, p.209(3)] に対応して

公式 10 $L_N^{AB}(x+y) = \frac{q}{q-1} \sum_M L_M^A(x) L_{N\overline{M}}^B(y)$ である。 ■

$L_n^a(xy) = \sum_{m=0}^{\infty} \frac{(1+a)_n}{(1+a)_m (n-m)!} (1-y)^{n-m} y^m L_m^a(x)$ [6, p.209(5)] に対応して

公式 11 $AN \neq 1, xy \neq 0$ ならば

$$ L_N^A(xy) = \frac{q}{q-1} \sum_M \frac{G(AN)}{G(AM)G(N\overline{M})} N\overline{M}(1-y) M(y) L_M^A(x) $$

$$ + N(y) L_N^A(x) + \frac{1}{q} \overline{A}(xy) AN(1-y) G(A) \quad \text{である。} $$ ■

3 Matrix elements of the representation ρ of G.

有限一般線型群 $GL(3,q)$ の部分群 G を次のようにとる。

$$G := \left\{ g = \begin{pmatrix} 1 & a & b \\ & c & d \\ & & 1 \end{pmatrix} \middle| \begin{array}{c} a,\ b,\ d \in \mathbb{F}_q \\ c \in \mathbb{F}_q^\times \end{array} \right\}$$

V を $\mathbb{F}_q$ 上の複素数値関数全体のなすベクトル空間とし、V における内積を $f, f' \in V$ に対して

$$\langle f, f' \rangle := \frac{1}{q-1} \sum_{z \in \mathbb{F}_q} f(z)\overline{f'(z)}$$

と定める。$\{\tilde{\delta}\} \cup \hat{\mathbb{F}}_q^\times$ は V の正規直交基底である。ただし

$$\tilde{\delta}(z) = \begin{cases} \sqrt{q-1} & (z = 0 \text{ のとき}) \\ 0 & (z \neq 0 \text{ のとき}) \end{cases} \quad \text{である。}$$

$\chi \in \hat{\mathbb{F}}_q^\times, \mu = {}^w\lambda_0 \in \hat{\mathbb{F}}_q^+ - \{1\} (w \in \mathbb{F}_q^\times)$ をとる。G の V への作用を

$g = \begin{pmatrix} 1 & a & b \\ & c & d \\ & & 1 \end{pmatrix} \in G, f \in V, z \in \mathbb{F}_q$ に対して

$$(g.f)(z) := \chi(c)\mu(b + dz) f(a + cz)$$

と定める。この作用による V の正規直交基底 $\{\tilde{\delta}\} \cup \hat{\mathbb{F}}_q^\times$ に関する行列表現を $\rho = \rho(\chi, \mu)$ とする。ρ は既約である。$g \in G$ に対して

$$\rho(g) = \left(\begin{array}{c|c} X^{\chi,\mu}(g) & Y_C^{\chi,\mu}(g) \\ \hline Z_B^{\chi,\mu}(g) & W_{B,C}^{\chi,\mu}(g) \end{array} \right)_{B,C \in \hat{\mathbb{F}}_q^\times}$$

と書く。このとき次の定理が成り立つ。

定理 1 (1) $X^{\chi,\mu}(g) = \chi(c)\mu(b)\delta(a)$

(2) $Y_C^{\chi,\mu}(g) = \dfrac{1}{\sqrt{q-1}} \chi(c)\mu(b)C(a)$

(3) $Z_B^{\chi,\mu}(g) = \dfrac{1}{\sqrt{q-1}} \chi(c)\mu\left(b - \dfrac{ad}{c}\right) \overline{B}\left(-\dfrac{a}{c}\right)$

(4) $W_{B,C}^{\chi,\mu}(g) = \begin{cases} \dfrac{q}{q-1} \chi(c)\mu(b)\overline{B}C(a)B(c)L_B^{\overline{B}C}\left(\dfrac{wad}{c}\right) & (a \neq 0 \text{ のとき}) \\ \dfrac{1}{q-1} \chi(c)\mu(b)C(c)B\overline{C}(wd)G(\overline{B}C) & (a = 0,\ d \neq 0 \text{ のとき}) \\ \chi(c)\mu(b)C(c)\delta_{B,C} & (a = 0,\ d = 0 \text{ のとき}) \end{cases}$

ただし $\delta_{B,C} = \begin{cases} 1 & (B = C \text{ のとき}) \\ 0 & (B \neq C \text{ のとき}) \end{cases}$ である。 ■

注意 2 G と V を一般化して、群 G_n とベクトル空間 V_n を次の様にとる。

$$G_n = \left\{ \begin{pmatrix} 1 & a_1 & \cdots & a_n & b \\ & c_1 & & & d_1 \\ & & \ddots & & \vdots \\ & & & c_n & d_n \\ & & & & 1 \end{pmatrix} \right\} \leq GL(n+2,q), \quad V_n = \{ f : \underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{n\text{個}} \longrightarrow \mathbb{C} \}.$$

G_n の V_n への作用、V_n の内積、基底、を上と同様に自然に与えると、定理 1 (4) の第 1 式は拡張され、Laguerre 和の積が現われる。

一般に, 行列表現の成分に関して次の補題が知られている。

補題 3 G を任意の有限群、ρ を G の n 次の既約行列表現とし、$g \in G$ に対して $\rho(g) = (r_{ij}(g))_{1 \leq i,j \leq n}$ と書くとき、次の関係式が成立する。

$$\sum_{g \in G} r_{ij}(g^{-1}) r_{kl}(g) = \frac{|G|}{n} \delta_{il} \delta_{jk}$$

■

この補題と定理 1 を使って、Laguerre 和に関する次の公式を得る。

系 4 $\displaystyle\sum_{x \in \hat{\mathbb{F}}_q} \zeta^x L_A^{\overline{A}B}(x) L_B^{\overline{B}A}(x) = \frac{q-2}{q} AB(-1)$ である。 ■

また次の命題が成り立つ。

命題 5 $g \in G, f, f' \in V$ に対して、$\langle g.f, g.f' \rangle = \langle f, f' \rangle$ である。 ■

これと定理 1 を使って次の公式を得る。

系 6 $\displaystyle\frac{q^2}{(q-1)^2} \sum_{C \in \hat{\mathbb{F}}_q^\times} L_A^{\overline{A}C}(x) \overline{L_B^{\overline{B}C}(x)} = \delta_{A,B} - \frac{1}{q-1} AB(-1)$ である。 ■

参考文献

[1] R. Evans, Hermite character sums, *Pacific J. Math.* 122(1986), 357-390.

[2] J. Greene, Hypergeometric functions over finite fields, *Trans. AMS* 301(1987), 77-101.

[3] J. Greene, Hypergeometric functions over finite fields and representations of $SL(2,q)$, *Rocky Mountain J. Math.*, 23(1993), 547-568.

[4] N. Lebedev, *Special Functions and Their Applications*, Dover, N.Y., 1972.

[5] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, Mass., 1983.

[6] E. Rainville, *Special Functions*, Macmillan, New York, 1960.

[7] N. Saito, Laguerre Character Sums, preprint.

[8] Y. Sawabe, Legendre character sums, *Hiroshima Math. J.* 22(1992), 15-22.

Possibility of dividing strongly regular graphs into two hyperplanes

Makiko Watanabe

Graduate school of Mathematics Kyushu University

1 Problem and the Motivation

Some coherent configuration has the structure that its embedding on concentric spheres satisfies the following conditions: (1) its embedding is on two concentric spheres and (2) on each sphere, it forms a strongly regular graph and for each point on a sphere, inner product with any point outside of the sphere has only two values.

Hence, it would be interesting to study strongly regular graphs related to condition (2) above. We state the problem as follows:

(*) For a given strongly regular graph, in an embedding (in some case in a Euclidean space of smaller dimension), find a vector with which the inner product has exactly two values.

We have partial results for this problem.

2 Some consequence for *

Definition 1 [Strongly regular graph (SRG)]

A strongly regular graph Γ is a connected regular graph (any vertex has the same number of adjacent vertices) with a property that for any two vertices x, y of Γ, the number of vertices which are adjacent to both of x and y depends only on whether x and y are adjacent or not, not on the choice of x and y.

Definition 2 [Johnson Scheme] For given numbers v, d, $(d \leq v/2)$, let $S = \{1, 2, \ldots, v\}$, $X = \{T \subset S \mid |T| = d\}$, and define the relation on X as $R_i = \{ (T_1, T_2) \in X \times X \mid |T_1 \cap T_2| = d - i\}$. Then $\mathcal{X} = (X, \{R_i\}_{i=0,1,\ldots d})$ is a symmetric association scheme and we call it *Johnson Scheme* $J(v, d)$.

Definition 3 [Hamming Scheme]

Let $F = \{1, 2, \ldots, q\}$, and $X = F^d$. For x, y in X, where $x = (x_1, x_2, \cdots, x_d)$ and $y = (y_1, y_2, \cdots, y_d)$, we define Hamming distance as $\delta(x, y) = \#\{j | x_j \neq y_j\}$. Define relations on X as $R_i = \{(x, y) \in X \times X \mid \delta(x, y) = i\}$. Then $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ is a symmetric association scheme, *Hamming scheme* $H(d, q)$.

Some association scheme with 2 classes are strongly regular graphs. The vertices of the graph are the points of X and $\{x, y\}$ is an edge if $(x, y) \in R_1$.

From now on, denote X to be the vertex set of the graph, A_i the adjacency matrix, and E_i the primitive idempotent of the adjacency algebra.

Theorem 1 *1. For $J(v, 2)$, when the graph becomes a SRG, all the vectors such that the innerproduct of the vector and each point of the graph has exactly two values can be written as $\sum_{x \in X_i} E_1 x$, where X_i is the 2-subset which includes i.*

2. For $H(2, q)$, when the graph becomes an SRG, all the vectors such that the innerproduct of the vector and each point of the graph has exactly two values can be written as $\sum_{x \in X_r^{(j)}} E_1 x$ where $X_r^{(j)} = \{x \in X \mid x = (x_1, x_2), x_j = r\}$.

(*Sketch of proof.*)

Pick up a set of linearly independent vectors $E_1 x_1, \ldots, E_1 x_{v-1}$. Write the vector that satisfies (*) as a linear combination of the above set of vectors. Then the inner product of the vector and the representatives of the graph has only two values. Solving this, we get the above vectors in Theorem 1. The important point here is to choose a good set of linearly independent vectors.

Remark

In general, for $J(v, d)$, let X_i be the collection of d-set of S which includes i in it, and let $u = \sum_{x \in X_i} E_1 x$. Then this vector divides the vertex set into two hyperplanes. And also for $H(d, q)$, let $X_r^{(j)} = \{x \in X \mid x = (x_1, \ldots, x_d), x_j = r\}$, $u_r^{(j)} = \sum_{x \in X_r^{(j)}} E_1 x$. Then for the subset $S \subset F$ $(S \neq F)$, $\sum_{r \in S} u_r^{(i)}$ for $1 \leq i \leq d$ divides the points X into two hyperplanes.

For $J(8, 2)$, there are three graphs which have the same parameters. These graphs are called *Chang graphs*.

Theorem 2 *Any Chang graph has no division of graph which satisfies* (*).

The above theorem says that (*) cannot be proved by parametrical condition. Now let us see a few other examples.

Definition 4 [Grassmann graph]

Let F be an arbitrary field. V a n-dim vector space over F, $\begin{bmatrix} V \\ d \end{bmatrix}$ be linear subspaces of V of dimension d.

The Grassmann graph is the graph whose vertex set $X = \begin{bmatrix} V \\ d \end{bmatrix}$, and adjacency is defined as $\gamma \sim \delta \Leftrightarrow \dim \gamma \cap \delta = d - 1$.

Let $F = GF(q)$.

In general, for Grassmann graph on $X = \begin{bmatrix} V \\ d \end{bmatrix}$, fix a 1-dimensional vector u in V, and let $X_u = \{\gamma \in X | u \in \gamma\}$. Then $v = \sum_{\gamma \in X_u} E_1 \gamma$ is a vector that divides the vertices of this graph into 2 hyperplanes.

We have some other examples on SRG's which have division satisfying (*). All the cases turned out that the vector which satisfies (*) is written as a sum of the points of the graph which have the same innerproduct with the vector. Therefore, the next theorem is a very natural description about (*).

Theorem 3 *Let Γ be a SRG and X be a vertex set. Then the following statements are equivalent*

1. *Let X_1 be a subset of X, and $X_2 = X - X_1$. Then the value of innerproduct of $\sum_{x \in X_1} E_1 x$ and the point of the graph is determined according to whether the point belongs to X_1 or X_2.*

2. *(a) For any point x in X_1, a number of points which are adjacent to x within X_1 is constant.*

   (b) For any point x in X_2, a number of points which are adjacent to x within X_2 is constant.

3. *X_1 is a 1-design or 1-antidesign.*

Remark

The above theorem does not prove every case of (*). The remaining problem is: Can all the vectors which make a division of the graph be described as a sum of some points of the graph?

References

[1] Bannai, Eiichi and Ito. Tatsuro. Algebraic Combinatorics I. California: Benjamin-Cummings, 1984.

[2] P.Delsarte, An algebraic approach of the association schemes of coding theory, Philips Res. Rep. Suppl. 10, 1973.

[3] C. Roos. On antidesigns and designs in an association scheme, Delft Prog. Rep., 7 (1982) pp. 98-109

[4] A. Neumaier, Regular sets and quasi-symmetric 2-designs, Combinatorial theory (Schloss Rauischholzhausen, 1982), pp. 258–275, Lecture Notes in Math., 969, Springer, Berlin-New York, 1982.

Higher Dimensional Dual Hyperovals

Satoshi Yoshiara (吉荒 聡)
Division of Mathematical Sciences
Osaka Kyoiku University

この記録は金沢大学工学部で１９９８年６月２４日に行われた筆者の講演のほぼ忠実な再現であるが、細部の説明も多少加味した。内容は、二次曲線の幾何学的特徴付けから生まれた超卵型 (hyperoval) という古典的概念の高次元版の一つの定式化を紹介し、それが組合せ論の新しい研究対象として期待出来そうなものであるという事実の説得を、最近の筆者や Del Fra の仕事の素描を通じて行う事である。

以下 q は素数のべきを表す。q 元体 $\mathbf{F}_q$ 上の $n+1$ 次元ベクトル空間 V の 1,2,3,...,n 次元部分空間の全体に包含関係を考えあわせた対象を $\mathbf{F}_q$ 上の n 次元射影空間と呼び $PG(V)$ あるいは $PG(n,q)$ と書く。V の i-次元の部分空間を $PG(n,q)$ の対象と見たときには $i-1$（射影）次元の部分空間といい、特に $0.1.2.n-1$ 次元の部分空間を点、直線、平面、超平面という。本稿では、以下特に断らぬ限り、次元と言ったときには射影次元を意味する。

高次元の双対超卵形–定義と動機

通常の hyperoval　$\mathbf{F}_q$ 上の射影平面 $PG(2,q)$ の $q+2$ 点からなる集合 $\mathcal{O}$ が *hyperoval*(超卵型とでも訳すべきか) と呼ばれるのは、

> (P)　$\mathcal{O}$ のどの相異なる 3 点を取っても、それらを通過する直線は存在しない

ことであった。この概念の dual（点と直線を取り替えて得られる構造）を考えれば、それは射影平面 $PG(2,q)$ 中の $q+2$ 本の直線からなる集合 $\mathcal{O}^*$ で、

> (P^*)　$\mathcal{O}^*$ のどの相異なる 3 直線を取っても、それらは一点では交わらない

ようなものの事である。これは *dual hyperoval* と呼ばれる。

次の事実は比較的簡単に示せる。「射影平面 $PG(2,q)$ の 点集合 $\mathcal{O}$ が上の性質 (P) を満たすならば $|\mathcal{O}| \leq q+2$ であり、q が 2 のべきであるとき、かつその時に限って $|\mathcal{O}| = q+2$ を満たす集合 $\mathcal{O}$ が存在する。」従って q が奇素数のべきのとき (P) を満たす点集合 $\mathcal{O}$ は高々 $q+1$ 点しか含み得ないが、$|\mathcal{O}| = q+1$ を満たす集合 $\mathcal{O}$ が次のように作れる。一般の素数べき q に対して射影平面 $PG(2,q)$ 中で非退化な二次多項式の零点の全体 (conic という) を考えれば、それは $q+1$ 点からなる "卵型"（通常の実平面では楕円か双曲線であるが、後者も直線の無限遠点の対を同一視すれば卵型である）をなし、上の性質 (P) を満たす。実は q が奇素数べきのときには、こういうものしか存在しない、つまり、「q が奇素数べきのときには、(P) を満たす $q+1$ 点よりなる集合のどれもが、適当な二次多項式の零点集合として得られる」というのが有名な Segre の定理である。これは平面上の二次曲線の美しい幾何学的特徴付けである。

一方、q が 2 のべきのときは事情は簡単ではない。一般に (P) を満たす $q+1$ 点の集合 $\mathcal{O}'$ があれば（例えば conic)、その各点における接線を取るとこれらのすべてがある共通の点 (nucleus と呼ばれる) を通過する事が示され、$\mathcal{O}'$ にその nucleus を併せたもの $\mathcal{O}$ が性質 (P) を満たす $q+2$ 点の集合である事が示される。それでは上の Segre の定理の拡張「すべての hyperoval $\mathcal{O}$ に対して、そこからうまく一点を抜き出せば、残りの $q+1$ 点は conic になる」が成り立つかと期待すると、一般にはそうではない。そうなっているときには $\mathcal{O}$ は classical (ないしは regular) という。

しかしながら、超卵型は、二次とは限らないある多項式（ある種の置換多項式）の零点集合にその nucleus を添加したものである事はすぐ示せる。そこで、classical でない hyperoval を見つけるという問題は置換多項式に関する有限体上の数論の問題に帰着される。この観点から、主としてオーストラリアの研究者を中心に、計算機を用いて観察された低次元の現象の一般化や、有限幾何の概念を巧妙に用いた記述という形で、様々な研究がなされている。このようにして非退化二次曲線の零点集合の拡張にならないような超卵形は、Segre が当初から気付いていたものの他に最近幾つかの無限系列が構成されている。([Th1] 参照）ただし、hyperoval を与える置換多項式の類は、とても分類出来るとは思えない。

高次元化への動機　以下解説したいのは、この hyperoval という概念の高次元への一般化である。（実際には、hyperoval よりもその dual を考えた方が定式化し易いので dual hyperoval の高次元版を考える。）私が期待しているのは、上記の Segre の定理の類似を示す事、classical に相当する対象の発見、そして、non-classical な例の系列の構成（高次元なので分類可能なようにも感じる）等である。第二の課題については、後で紹介する Translation dual hyperovals が $q=2$ の場合のそれであると思っている。更に、高次元化する事によって、通常の hyperoval に関する研究にも新たな視点を提供できれば望外の喜びである。ともかく研究してみると、存外面白い対象であるし、今のところ、あまり知識がなくても一定の成果が得られるという利点（欠点？）もある。有志の参加を望む。

以下に述べる定式化が行われたのは極めて最近（１９９７年の秋頃、Pasini によるものと思われる）の事であるが、その動機となったのは、筆者による EGQ (extended sual generalized quadrangles) と呼ばれるある幾何構造の無限系列の構成である。(EGQ が何故重要か等、この辺の概観を掴むには [Yo2] を参照されたい。）これらの EGQ は 5 次元射影空間 $PG(5,q)$（ただし $q=2^e$）中のある性質を持つ $q+3$ 個の平面の族 $\mathcal{Y}$ から、そのアフィン拡大（幾何での一つの標準的手段）として構成できる。このような平面族 $\mathcal{Y}$ の構成は筆者が Veronese 写像を用いて与え [Yo1] 、Thas [Th2] が Klein 対応を用いて与えた。（この二つの構成が同じ平面族を与えるのは、関連して得られる通常の hyperoval が classical であるときしかない [Yo1] 。）この平面族は、

そのメンバーである平面達のどの二つの交わりを考えても、それは点である

という特徴を持っている。筆者は $q=2^e=4$ のときに構成した $\mathcal{Y}$ が、更に大きな（$q^2+q+2=22$ 個の平面からなる）族 $\mathcal{M}$ で同じ性質を持つものに含まれる事を発見

し、しかも $GL(6,q)$ の元で $\mathcal{M}$ を全体として保つもの達のなす群を考えると、それは $\mathcal{M}$ 上に 22 次 Mathieu 群を引き起こすことを確認した。

上の性質を持つ射影空間の（指定された次元の）部分空間の族を統一的に扱う試みの中から生まれたのが、higer dimensional dual arc（高次元の双対弧）という概念であり、その特別な場合として本稿の主題である higher dimensional dual hyperovals (高次元の双対超卵形) が定義される。

定義（高次元の双対弧） 有限体 $GF(q)$ 上の m 次元射影空間 $PG(m,q)$ の d-（射影）次元部分空間の族 S が *d-dimensional dual arc in $PG(m,q)$* であるとは、次の 4 条件が満たされる事を言う。

(a) $PG(m,q)$ のどの点に対しても、それを含む S のメンバーは高々 2 個である。換言すれば、S の相異なる 3 個のメンバー X,Y,Z について、つねに $X\cap Y\cap Z=\emptyset$ である。

(b) S の相異なる 2 個のメンバー X,Y に対し $X\cap Y$ は射影点である。

(c) S のどのメンバー X についても、これと他のメンバーとの交わりを考えれば、その全体は X を生成する。$X=\langle X\cap Y \mid Y\in S\setminus\{X\}\rangle$

(d) S のメンバー全体は $PG(m,q)$ を生成する。$PG(m,q)=\langle X \mid X\in S\rangle$

重要なのは条件 (a),(b) であり、(c) は補助的である。(a),(b),(c) が満たされれば S は射影空間 $\langle X \mid X\in S\rangle = PG(m',q)$ $(m'\le m)$ における dual arc をなす。

S のメンバー X を一つ取って固定すると、$S-\{X\}$ の各メンバー Y に対して $X\cap Y$ は条件 (b) から X 上の射影点であるが、逆に X 上の射影点 P を与えたとき、$X\cap Y=P$ を満たす S のメンバー Y は条件 (a) により高々 1 個存在する。従って、次の不等式を得る。等号が成立するのは、X 上のどの射影点 P についても、$X\cap Y=P$ を満たす S のメンバー Y が丁度 1 個存在するときであり、かつその時に限る。

$$|S|\le (q^d+q^{d-1}+\cdots+1)+1.$$

この不等式で等号が成立する場合に S を dual hyperoval と呼ぶ。換言すれば、

定義（高次元の双対卵型） 有限体 $GF(q)$ 上の m 次元射影空間 $PG(m,q)$ の d-次元部分空間の族 S が *d-dimensional dual hyperoval in $PG(m,q)$* であるとは、次の 3 条件が満たされる事を言う。

(a') $PG(m,q)$ のどの点に対しても、それを含む S のメンバーは 0 個か 2 個である。

(b) S の相異なる 2 個のメンバー X,Y に対し $X\cap Y$ は射影点である。

(d) S のメンバー全体は $PG(m,q)$ を生成する。$PG(m,q)=\langle X \mid X\in S\rangle$

dual hyperoval においては、dual arc の条件 (c) は自動的に満たされている事に注意されたい。

この対象を（高次元の）dual hyperoval と呼ぶのは $d=1$ のときには、確かに従来の dual hyperoval の概念と一致するからである：実際に、$d=1$ として S の異なる二つのメンバー X,Y を取る。このとき $S-\{X,Y\}$ の任意のメンバー Z は 1-subspace（射影直線）であるから、二つの射影点 $X\cap Z$ と $Y\cap Z$ により生成され、特に $Z\subseteq\langle X,Y\rangle$ である。従って 条件 (d) から $PG(m,q)=\langle S\rangle=\langle X,Y\rangle$ であり、$m=2$ となる。しかも、このとき S は射影平面 $PG(2,q)$ 中の $(q+1)+1=q+2$ 本の射影直線の集合で、そのうちのどの異なる 3 本も一点で交わることはない（条件 (a') から）、ようなものである。従って 1-dimensional dual hyperoval S は、射影平面中の通常の hyperoval に他ならない。特に $d=1$ のときには q が 2 のべきであることが結論される。

高次元双対超卵型の一般的性質

先にも殆ど述べたことであるが、先ず次に注意する。

事実 1 $PG(m,q)$ の d-次元部分空間の集合 S が d-dimensional dual hyperoval である為の必要かつ十分な条件は、dual arc の条件 (a),(b),(d) 及び $|S|=q^d+\cdots+q+2$ が満たされることである。

m と d の関連については、今のところ、次の簡単な結果しか知られていない。

事実 2 – m の上限 (Del Fra [DF], 1998) $PG(m,q)$ 中の d-次元双対超卵型が存在すれば

$$(*)\quad m<2d+\textstyle\sum_{i=1}^{d-1} iq^{d-i}$$

$m\leq 2d+\sum_{i=1}^{d-1} iq^{d-i}$ であることは次のように簡単に分かる。$m\neq 2d+\sum_{i=1}^{d-1} iq^{d-i}$ であることの証明に関しては [DF, Prop. 2. 5] を参照。

S を $PG(m,q)$ 中の d-次元双対超卵型とする。初めに $PG(m,q)$ は S の $q^d+\cdots+q+2$ 個のメンバー全部を持ってくる必要はなく、その $r:=q^{d-1}+\cdots+q+2$ 個のメンバー $X_1,\ldots,X_r$ によって生成される事に注意する：実際、これらが生成する射影部分空間を $U:=\langle X_1,\ldots,X_r\rangle$ とする。S の $X_1,\ldots,X_r$ 達と異なる任意のメンバー X に対して、$X\cap X_i\,(i=1,\ldots,r)$ という r 個の異なる点が $X\cap U$ に入る。ところで d-次元射影空間 X の部分空間 $X\cap U$ の次元が $(d-1)$-次元以下ならば、高々 $q^{d-1}+\cdots+1\,(<r)$ しか含み得ないので、$X\cap U=X$ すなわち $X\subseteq U$ である。従って $PG(m,q)=\langle X\mid X\in S\rangle=U$ となる。

さて、まず S の 2 個のメンバー X_1,X_2 の生成する空間 $U_2:=\langle X_1,X_2\rangle$ の射影次元は、$X_1\cap X_2$ が射影点であるから、$\dim U_2=2d$ である。ここに第三のメンバー X_3 を付け加えて生成される空間 $U_3:=\langle X_2,X_2,X_3\rangle$ の射影次元は

$$\begin{aligned}&\dim U_3=\dim U_2+\dim X_3-\dim(U_2\cap X_3)\\&\leq\dim U_2+d-\dim\langle X_1\cap X_3,X_2\cap X_3\rangle=2d+d-1\end{aligned}$$

と評価される。ここで部分空間 $U_2 \cap X_3$ の次元を下から評価するため、この空間に含まれる 2 個の射影点 $X_1 \cap X_3$, $X_2 \cap X_3$ の生成する部分空間 $I_3 := \langle X_1 \cap X_3, X_2 \cap X_3 \rangle$ に置き換えている。これは明らかに射影直線である。同様に $U_4 := \langle X_1, \ldots, X_4 \rangle$ の次元も

$$\begin{aligned} &\dim U_4 = \dim U_3 + \dim X_4 - \dim(U_3 \cap X_4) \\ &\leq \dim U_3 + d - \dim \langle X_1 \cap X_4, X_2 \cap X_4, X_3 \cap X_4 \rangle \leq \dim U_3 + d - 1 \end{aligned}$$

と評価される。ここで部分空間 $U_3 \cap X_4$ の次元を下から評価するため、この空間に含まれる 3 個の射影点 $X_i \cap X_4$ $(i = 1, \ldots, 3)$ の生成する部分空間 $I_4 := \langle X_i \cap X_4 | i = 1, 2, 3 \rangle$ に置き換えているのだが、I_4 の射影次元は最低 1 であるので、最後の評価式が得られる。

このようにして続けていくと $3 \leq j \leq q+2$ までは $I_j = \langle X_i \cap X_j | i = 1, \ldots, j-1 \rangle$ は高々 $q+1$ 個の射影点で生成されているから、その次元は最低 1 であるが、$q+3$ になると I_{q+3} は $q+2$ 点を含むので、その次元は最低 2 となる。$q+3 \leq j \leq q^2+q+2$ においては同様に $\dim(I_j) \geq 2$ という状態が続き、次に q^2+q+3 になると I_{q^2+q+3} は q^2+q+2 点を含むので、その次元は最低 3 となり、$q^2+q+3 \leq j \leq q^3+q^2+q+3$ においては $\dim(I_j) \geq 3$ と評価される。

以上の事を頭にいれて 評価式

$$\dim(U_j) \leq \dim(U_{j-1}) + d - \dim(I_j)$$

を $j = 2$ から $q^{d-2} + \cdots + q + 2 = r$ まで加えあわせれば、$U_r = PG(m,q)$ であったから、m を q, d で評価する式（上の $(*)$ で等号を含んだもの）が得られる。

問題 1　この上限 $(*)$ をもっと鋭いものにせよ。

q の偶奇について　通常の dual hyperoval が存在するのは q が 2 のべきのときに限られていたが、高次元の場合はどうか？というと、今のところ、次の結果しか知られていない。（特殊な場合のもう少し細かい結果については [DF] 参照。）

事実 3.1　(Del Fra [DF], 1998) d を奇数とする。$PG(m,q)$ 中の d-次元双対超卵型が存在すれば、q は 2 のべきである。

事実 3.2　(Del Fra [DF] 及び Cooperstein-Thas [CT], 1998) $PG(2d,q)$ 中の d-次元双対超卵型が存在すれば、q は 2 のべきである。

ここでは事実 3.1 の証明を述べる。$d = 1$ ならば、これは良く知られている事だから、$d > 1$ としてよい。S を $PG(m,q)$ 中の d-次元の双対超卵型とする。はじめに、d の偶奇に無関係な次の事実に注意しよう。

S のどのメンバーも含まない $PG(m,q)$ の超平面が存在する。

実際、$PG(m,q)$ の一つの d 次元部分空間 X に対して X を含む超平面の個数は、商ベクトル空間 $GF(q)^{m+1}/GF(q)^{d+1}$ の m 次元部分空間の総数 $(q^{m-d}-1)/(q-1)$ に等し

い。そこで S のメンバーである d 次元部分空間 X_i $(i=1,\ldots,q^d+\cdots+q+2)$ のどれかを含む超平面の個数は、高々 $(q^{m-d}-1)/(q-1)\times(q^d+\cdots+q+2)$ 個であるが、簡単な計算により、これは超平面の総数 $(q^m-1)/(q-1)$ より真に小さい事が分かる。従って、S のどのメンバーも含まない超平面が存在する。

そこで U を $PG(m,q)$ の超平面で、すべての $X\in S$ に対して $X\not\subseteq U$ を満たすものとし、固定する。すると各 $X\in S$ に対して $X\cap U$ は X の超平面だから $(d-1)$-次元部分空間であり、しかも $X\neq Y\in S$ ならば $(X\cap U)\neq(Y\cap U)$ である。(実際、$X\cap U=Y\cap U$ ならば、$(d-1)$-次元部分空間 $X\cap U$ は射影点 $X\cap Y$ に含まれるので $d\leq 1$ となり、仮定に反する。) そこで $S':=\{X\cap U \mid X\in S\}$ を考えると $|S'|=|S|=q^d+\cdots+q+2$ である。しかも、S が超双対卵型であるから、次が成り立つ事がすぐ確認できる。(ここまでも d の偶奇に関係なく成立する。)

> S' は $PG(m-1,q)$ 中の $(d-1)$-次元の "弱" 超双対卵型である。すなわち、S' は $PG(m-1,q)$ 中の $(d-1)$-次元部分空間の族であって次を満たす。(第1節の超双対卵型の定義と比べられよ。)
>
> (a') $PG(m,q)$ のどの点に対しても、それを含む S のメンバーは 0 個か 2 個である。
>
> (b') S' のどの 2 個の相異なるメンバーの交わりも、射影点ないしは空集合である。
>
> (d) $\langle X \mid X\in S'\rangle = PG(m-1,q)$ である。

さて S' の相異なる二つのメンバーの交わり $(U\cap X\cap Y)$ $(X\neq Y\in S)$ として得られる射影点の総数を勘定する。S' の各メンバー $U\cap X$ について、その各点を通るような $S'-\{U\cap X\}$ のメンバー $U\cap Y$ がただ一つ存在する。(実際、$U\cap X$ の各点を通るような $Y\in S-\{X\}$ がただ一つ存在して $U\cap Y\in S'$ である。) 従って、上のような射影点の個数は

$$|\cup_{X\neq Y\in S}(U\cap X\cap Y)| = |S'|(q^{d-1}+\cdots+q+1)/2$$

である。

ここで初めて d が奇数だという仮定を使う。すると q の偶奇によらず、$(q^{d-1}+\cdots+q+1)$ は奇数である。従って、上の式から 2 は $|S'|=|S|=q^d+\cdots+q+2$ を割り切る。従って、q は偶数でなければならない。(一般に $q^i+\cdots+q+1$ は q が奇数であるか q が偶数で i が偶数ならば奇数、q が偶数で i が奇数のときのみ偶数である。)

理屈は非常に簡単だという事が納得できるであろう。また、もう少し追求する事が出来そうであるという気にもなるであろう。事実 3.2 の証明については [DF] を見られたい。

さて、上の事実を見ると自然に次の問が生じるが、これは高次元双対超卵型に関する主問題の一つである。

問題 2 d を偶数, q を奇素数のべきとするとき $PG(m,q)$ 中の d-次元双対超卵型が存在するか？ このような例を構成するか、非存在を示せ。

高次元双対超卵型の例と分類の試み

以下 $d > 1$ とする。実は余り多くの例は知られていない。

例 1 (Cooperstein-Thas [CT], 1998) すべての d について $PG(2d,2)$ 中の d-次元双対超卵型が存在する。

ここでは具体的な構成の説明は省くが、興味のある人は [DF, 1.2] に記述があるので、それを参照のこと。重要な事は、この例は「$PG(2d,2)$ 中の d-次元双対超卵型 S であって、そのどのメンバーにも含まれないような $PG(2d,2)$ の射影点全体が一つの $(d-1)$-次元部分空間をなす」という事実により特徴づけられる、という点である。

一般に $PG(m,q)$ 中の d-次元超卵型 S のどれかのメンバーに含まれる射影点の個数は

$$|\cup_{X \neq Y \in S} (X \cap Y)| = |S|(|S|-1)/2 = (q^d + q^{d-1} + \cdots + q + 2)((q^d + q^{d-1} + \cdots + q + 1)/2$$

で与えられる。(前節の事実 3.1 の証明中の説明参照。) 特に $q = 2$ のときには $2^d + 2^{d-1} + \cdots + 2 + 1 = 2^{d+1} - 1$ だから、この数は

$$|\cup_{X \neq Y \in S} (X \cap Y)| = 2^d(2^{d+1} - 1)$$

となる。そこで $PG(2d,2)$ 中の d-次元双対超卵型のどのメンバーにも含まれないような $PG(2d,2)$ の射影点の総数は $(2^{2d} + \cdots + 1) - (2^d(2^{d+1}-1) = (2^{2d+1}-1) - (2^{2d+1} - 2^d) = 2^d - 1$ となる。この結果は、$PG(2d,2)$ 中のどんな d-次元双対超卵型についても、このような射影点の全体が一つの $(d-1)$-次元部分空間をなす事を期待させる。

実際にそうなっている事は Del Fra により確かめられた。([DF, Prop. 3. 1]) 従って、この Del Fra の結果と Cooperstei-Thas の例の特徴付けをあわせれば、「$PG(2d,2)$ 中の d-次元双対超卵型はすべて Copperstein-Thas の構成法により構成される」という事実が成り立っている。

例 2 第 1 節で述べた $PG(5,4)$ 中の 2-次元部分空間の族 $\mathcal{M}$ は $PG(5,4)$ 中の 2-次元双対超卵型である。しかも、そこで注意したように $Aut(\mathcal{M}) := \{\sigma \in Aut(PG(5,4)) \mid \mathcal{M}^\sigma = \mathcal{M}\}$ は 22 個の $\mathcal{M}$ のメンバー上に 22 次 Mathieu 群を引き起こし、従って二重可移に作用している。

実は、$PG(m,q)$ 中の d-次元双対超卵型 S で、その上に自己同型群 $Aut(S) := \{\sigma \in Aut(PG(m,q)) \mid S^\sigma = S\}$ が二重可移に作用するようなものは、Huybrechts と Pasini により分類されている [HP](1998):結果を言えば、そのようなものがあるとすれば ($d > 1$ としたことに注意) $q = 2$ であるか、$Aut(S)$ 中に Singer cycle $GL_1(q^m)$ が normal subgroup として含まれるか、または S が先の例 2 の $\mathcal{M}$ に一致するか、のどれかである。

この結果は、非可解で十分大きい自己同型群を持つような高次元の dual hyperoval が期待できるのは $q = 2$ (と $q = 4$) に限られることを示す。この結果の現証明は、二重可移群の分類 (これは有限単純群の分類を必要とする) と flag-transitive linear space の分類 (これも有限単純群の分類を必要とする) を初めから本質的に用いている。もう少

し弱い結論しか得られなくても良いから、組合せ論的考察を補助に用いてより初等的な証明を考えるのも、色々発展できる方法を生む可能性があり、面白い試みかも知れない。

また、群論的条件を付けずに幾つかの分類結果が得られている。

一つは Del Fra による 2-次元双対超卵型の分類の試みである：$PG(m,q)$ 中に 2-次元双対超卵型が存在すれば、$m=4$ または 5 であり、q は 2 のべきである。[DF, Prop. 4. 1, 4. 3] 更に $q=2$ と仮定したとき、$PG(4,2)$ 中の 2-次元双対超卵型は同型を除いて 2 個存在し、$PG(5,2)$ 中の 2-次元双対超卵型も同型を除いて 2 個存在する。[DF, Theo. 1, 2] 更に $q=4$ のときには次の幾何的条件 (Property (T)) を満たす $PG(5,4)$ 中の 2-次元双対超卵型は、先の例 2 の $\mathcal{M}$ に同型となる。[DF, Theo. 3] ここで d-次元双対超卵型 S が *Property (T)* を満たすとは、S のどの 3 個の相異なるメンバー X,Y,Z を取っても $\langle X,Y\rangle \cap Z$ が射影直線となることとする。

もう一つは Huybrechts による Property (T) を満たす d-次元双対超卵型に関する結果 [Hu] で、それは $PG(m,q)$ 中に Property (T) を満たす 2-次元双対超卵型が存在すれば $q=2$ または 4 というものである。従って、上の Del Fra の分類結果を見ると、$PG(m,q)$ 中の Property (T) を満たす 2-次元双対超卵型は $PG(5,2)$ 中に一つ (これは後で言う $\mathcal{S}_1^1$ に同型)、$PG(5,4)$ 中に一つ ($\mathcal{M}$ と同型) あるという結果になる。

高次元双対超卵型の新しい例

今年 4 月 2 7 日を過ぎた頃、ふと $q=2$ に対する dual hyperoval を作ってみようと思い立った筆者は、好運にも数日のうちに $PG(2d+1,2)$ 中の d-次元双対超卵型の無限系列を見いだすことが出来た。その後、その自己同型群・同型性等を考察してみると（これらは一般の組合せ構造についてはそんなに簡単な問題ではないが）、うまい具合に解決できたので、ここに報告する。詳細については [Yo3] を見られたい。

金沢で述べた時点では、同型問題について一つ残っていた場合があったが、これは解決した。またその時点の証明の中には、不完全なものがあることが Pasini により指摘されたが、現在ではより分かりやすい形の完全な証明に改良された。

5 月 2 日に新たな例について報告したとき即座に関心を持って色々な問題提起をしてくれた Del Fra 氏、5 月 23 日にこの例の構成について近畿大学のゼミで発表したとき、同型問題の解決のための有効な示唆を与えてくれた Kantor 氏、7 月 5 日版の preprint を精読して詳細にわたる notes を送ってくれた Pasini 氏等の好意に深く感謝したい。

構成 (Yoshiara, May 2, 1998) $q=2^e$ とし、q 元体 $GF(q)$ を $GF(2)$ 上の e-次元ベクトル空間と見る。$GF(q)$ の元の対の全体を

$$V := \{(x,y) \mid x,y \in GF(q)\}$$

とおき、これを $GF(2)$ 上の $2e$ 次元ベクトル空間と見る。e と互いに素である整数 m, $1 \le m \le e-1$ を取り固定する。対 $(a,b) \in V$ に対して V の e-次元部分空間 $X(a,b)$ を

$$X(a,b) := \{(x, x^{2^m}a + xb) \mid x \in GF(q)\}$$

により定める。$d := e-1$ とおくと V の定める射影空間 $PG(V)$ は $GF(2)$ 上の $2d+1$ 次元射影空間であり、$X(a,b)$ はその d-次元部分空間である。

さて V の部分集合 C を次の条件を満たすように取る。

(1) $(a,b) \neq (a',b') \in C$ ならば $a \neq a'$ かつ $b \neq b'$.

(2) C のどの 3 元も一直線上には存在しない。

(3) $|C| = q$.

このような集合は非常に多く存在する。実際、V を射影平面 $PG(2,q)$ から一直線 l_∞ を取り除いた集合だと見ると、$PG(2,q)$ の通常の oval O (そのどの 3 元も一直線上には存在しないような $q+1$ 点からなる集合) から一点 $O \cap l_\infty$ を除いた集合 C は上の条件を満たす。

このとき次が簡単に検証できる。

$S_m(C) := \{X(a,b) \mid (a,b) \in C\}$ は $GF(2)$ 上の射影空間
$\langle X(a,b) \mid (a,b) \in C \rangle$ における d-次元の双対超卵型である。

実際、$X(a,b) \cap X(a',b')$ 中に零ベクトルでない (x,y) が存在するのは $y = x^{2^m}a + xb = x^{2^m}a' + xb'$ すなわち $(b+b')/(a+a') = x^{2^m-1}$ を満たす $x \in GF(q)^*$ が存在するときに限るが、C の条件 (1) によりこのような x は存在し、$(m,e) = 1$ より唯一である。つまり $S_m(C)$ の異なる二つのメンバー $X(a,b)$ と $X(a',b')$ の交わりは射影点 であり、第 1 節の条件 (b) が満たされる。

3 個の異なるメンバー $X(a,b)$, $X(a',b')$, $X(a'',b'')$ が一点で交わるとすれば、上の式から $(b+b')/(a+a') = (b+b'')/(a+a'')$ となるが、これは C の元 (a,b), (a',b'), (a'',b'') が同一直線上に位置することを示し、C の条件 (2) に反する。従って、$S_m(C)$ の 3 個の相異なるメンバーの交わりは（射影部分空間と見て）空集合であり、第 1 節の条件 (a) が満たされる。

更に、第 1 節の条件 (c) は自明に満たされており、

$$|S_m(C)| = q = 2^e = (2^e - 1) + 1 = (2^{e-1} + 2^{e-2} + \cdots + 2 + 1) + 1$$

であるから、$d = e-1$ であったことに注意すると、d-(射影) 次元部分空間の集合 $S_m(C)$ は、確かに $GF(2)$ 上の射影空間 $\langle X(a,b) \mid (a,b) \in C \rangle$ における d-次元の双対超卵型である。

Translation dual hyperoval (平行移動不変な超卵型) そこで $\langle X(a,b) \mid (a,b) \in C \rangle$ の次元が問題になる。これをはっきり求めるためには、C の形を指定する必要がある。ここでは次のような集合を選ぶ。

h を e と互いに素で $1 \leq m \leq e-1$ を満たす整数とし、
$C_h := \{(t, t^{2^h}) \mid t \in GF(q)\}$ とする。

このとき C_h が C に関する条件 (1),(2),(3) を満たすことは容易に確認される。以下 $S_m(C_h)$ のことを簡単に S_m^h と書いて、*translation dual hyperoval* (平行移動不変な超卵型) と呼ぶ。

この命名の理由は、C_h が traslation oval と呼ばれる、平行移動を自己同型に持つ卵型から得られるからであるが、そればかりではなく、同様の事実が高次元の超卵型 S_m^h についても成り立つからでもある。すなわち、S_m^h には次のような自己同型が存在する : (Yos. May 16, 1998) V の元 (x,y) 及び $a \in GF(q)$, $b \in GF(q)^\times$, $\sigma \in Gal(GF(q)/GF(2))$ に対して

$$t_a : (x,y) \mapsto (x, x^{2^m}a + xa^{2^h} + y) \quad (\text{平行移動})$$

$$m_b : (x,y) \mapsto (xb, xb^{(2^{m+h}-1)/(2^h-1)}) \quad (\text{積})$$

$$f_\sigma : (x,y) \mapsto (x^\sigma, y^\sigma) \quad (\text{体同型})$$

により定められる $GF(2)$-線形変換 t_a, m_b, f_σ は S_m^h のメンバー $X(t) := X(t, t^{2^h})$ $(t \in GF(q))$ 上に次の置換を引き起こし、従って $Aut(S_m^h)$ の元である。

$$t_a : X(t) \mapsto X(t+a),\ m_b : X(t) \mapsto X(b^{(2^m-1)/(2^h-1)}t),\ f_\sigma : X(t) \mapsto X(t^\sigma)$$

特に $Aut(S_m^h)$ はこれらの変換が生成する部分群

$$\langle t_a \mid a \in GF(q)\rangle : (\langle m_b \mid b \in GF(q)^\times\rangle : \langle f_\sigma \mid \sigma \in Gal(GF(q)/GF(2))\rangle)$$
$$\cong GF(q) : (GF(q)^\times : Gal(GF(q)/GF(2))) \cong A\Gamma L_1(q)$$

(一次元半線形アフィン変換群) を含み、従って S_m^h 上に二重可移に作用する。

更に $\left\langle S_m^h \right\rangle = \langle X(t) \mid t \in GF(q)\rangle$ に関しては次を得る。ここで Tr は絶対トレース $Tr_{GF(q)/GF(2)}$ を表す。

$h+m \neq e$ ならば $\langle X(t) \mid t \in GF(q)\rangle = V$ であり、
$h+m = e$ ならば $\langle X(t) \mid t \in GF(q)\rangle$ は V の超平面
$W = \{(x,y) \in V \mid Tr(y) = 0\}$ に一致する。

従って、$e-1 = d$ としていた事に留意すれば、次がいえた。(Yos. May 5, 1998)

$h+m \neq e$ ならば S_m^h は $PG(2d+1,2)$ 中の d-次元双対超卵型であり、
$h+m = e$ ならば S_m^h は $PG(2d,2)$ 中の d-次元双対超卵型である。

そこで、$m+h \neq e$ という generic case においては、S_m^h は「$PG(2d+1,2)$ 中の d-次元双対超卵型」という新しい双対超卵型の系列を与える。一方、$m+h = e$ の場合には、S_m^{e-m} は前節例 1 で解説したように、Cooperstein-Thas の構成によって得られる双対超卵型でもあり、新しいものではない。

S_m^h の諸性質 Translation dual hyperoval S_m^h については、その具体的かつ簡明な構成の故に色々な性質が調べ易い。

(1) 同型性　一般に、同じ射影空間 $PG(m,q)$ 中の同じ次元 d の d-次元双対超卵型 S と S' が同型であるとは、$Aut(PG(m,q))$ の元 τ で $(S)^\tau = S'$ を満たすものがある事を言う。

$q=2$ のときには $Aut(PG(m,q)) = PGL_{m+1}(2)$ だから、$PG(m,2)$ を与える $m+1$ 次元のベクトル空間 $V = \langle S \rangle = \langle S' \rangle$ の全単射線形変換 τ で $(S)^\tau = S'$ を満たすものがある、といっても同じである。

命題　$e>2$ を整数とし m,h,n,k を 1 と $e-1$ の間の整数で e とは互いに素なものとする。このとき

(1) (Yos. May 25, 1998) $m+h \neq e$ かつ $n+k \neq e$ ならば $PG(2e-1,2)$ 中の $(e-1)$-次元双対超卵型 $\mathcal{S}_m^h$ と $\mathcal{S}_n^k$ が同型であるのは $m=n$ かつ $h=k$ であるか、$m+n=e$ かつ $h+k=e$ のとき、かつその時に限る。$m+n=e$ かつ $h+k=e$ のときの同型写像は

$$V \ni (x,y) \mapsto (x, y^{2^n}) \in V$$

により与えられる。

(2) (Yos. June 25, 1998[1]) $m+h=e$ かつ $n+k=e$ ならば $PG(2e-2,2)$ 中の $(e-1)$-次元双対超卵型 $\mathcal{S}_m^{e-m}$ と $\mathcal{S}_n^{e-n}$ はつねに同型である。同型写像は $x,z \in GF(q)$ に対して

$$W \ni (x, z^{2^m}+z) \mapsto (x, z^{2^n}+z) \in W$$

により与えられる。($\mathcal{S}_m^{e-m}$ らが生成するのは V の超平面 $W = \{(x,y) | x,y \in GF(q), tr(y)=0\}$ であり、$GF(q)$ の元 y が $tr(y)=0$ を満たせば $y = z^{2^m}+z$ と書ける事に注意。またこの写像が well-defined である事も確認される。)

Generic な場合 ($m+h \neq e$ かつ $n+k \neq e$) の結果の証明の鍵は、もし $\mathcal{S}_m^h$ から $\mathcal{S}_n^k$ への同型写像があれば、同型写像 τ として、

(1) $\mathcal{S}_m^h$ のメンバー $X_m^h(0)$ を $\mathcal{S}_n^k$ のメンバー $X_n^k(0)$ に移し (実は $X_m^h(0) = X_n^k(0) = \{(x,0) | x \in GF(q)\}$)、かつ、

(2) $Aut(\mathcal{S}_m^h)$ の積 m_b ($b \in GF(q)^\times$) のなす群 M_m^h を $Aut(\mathcal{S}_n^k)$ の積 m_b ($b \in GF(q)^\times$) のなす群 M_n^k に移す

ようなものが存在する、という事実である。実際、この注意と更に $\{(0,y) | y \in GF(q)\}$ という部分空間の像の可能性を考える事によって、可能な同型写像の形が殆ど限定されてしまい、後は、巡回群 M_m^h の生成元が巡回群 M_n^k のどの様な生成元に移るかを観察して得られる合同式を解くと、上の結果が得られる。(詳細は [Yo3, Prop. 11] 参照)

さて、(1) を満たすような同型写像の存在は $Aut(\mathcal{S}_n^k)$ の可移性からすぐ分かるが、更に (2) を満たすようにもできる点は Kantor が 5 月 23 日の私の話の直後に指摘してくれた。これは Sylow の定理に他ならない：というのは、まず、(1) を満たす $Aut(\mathcal{S}_m^h)$ の元

[1] これは金沢で話したときには未解決で問題 3 としたが、翌日に解決した

全体のなす群 A_m^h ($Aut(\mathcal{S}_m^h)$ における $X_m^h(0)$ の stabilizer) は $X_m^h(0)$ 上に faithfull に作用する（従って $GL_e(2)$ の部分群と同型）という事実が確認できる。A_n^k についても同様。

さて、積 m_b ($b \in GF(q)^\times$) のなす群 M_m^h は A_m^h の部分群で、その位数は $q-1 = 2^e-1$ に等しいから、$e=6$ のとき以外は 2^i-1 ($i=1,\ldots,e-1$) とすべて互いに素であるような 2^e-1 の素因子 p が存在する。$GL(V) \cong SL_e(2)$ の位数の公式を想起すれば、M_m^h は A_m^h の Sylow p-subgroup P_m^h を含んでいる。また、M_m^h は A_m^h を含む $GL_e(2)$ 中の Singer cycle であるから、その centralizer $C_{A_m^h}(P_m^h)$ は M_m^h に一致する。同様に M_n^k は A_n^k の Sylow p-subgroup P_n^k を含み、$C_{A_n^k}(P_n^k) = M_n^k$ である。

そこで (1) を満たす写像 τ を取ると、$(A_m^h)^\tau = A_n^k$ であるが、P_m^h の像 $(P_m^h)^\tau$ は位数 p の A_n^k の部分群なので Sylow の定理によって 適当な $g \in A_n^k$ を取れば $(P_m^h)^{\tau g} = P_n^k$ となる。従って τg は A_m^h における P_m^h の centralizer M_m^h を A_n^k における P_n^k の centralizer M_n^k に移す。写像 τg は条件 (1),(2) を満たす同型写像となる。（$e=6$ のときは多少個別の議論が必要だが、このときも Singer cycle の共役性に帰着する。）

(2) 自己同型　既に $Aut(\mathcal{S}_m^h)$ は $A\Gamma L_1(q)$ を含む q 個の d-次元部分空間の集合 $\mathcal{S}_m^h$ 上の二重可移群である事が分かっている。$Aut(\mathcal{S}_m^h)$ における $X(0)$ の stabilizer は先に注意したように $GL_e(2)$ の部分群で、Singer cycle M_m^h (位数 $q-1$ の巡回群) を含むものであったから、このような群の分類結果 [Ka](これは Cameron-Kantor による antiflag-transitive な射影平面の分類に帰着され、ここには有限群の分類定理は一切必要ではない) が使える。しかしながら $GL_d(2^{e/d})$ の形の部分群が生じる可能性をどの様に消すのか (特に $d=2$ のとき) については、それなりの着想が必要である。一般に $\mathcal{S}_m^h$ の自己同型の固定する射影点の集合が非常に特殊なものである事が導かれるので、それから色々な情報が導ける。(詳細は [Yo3, Lemma 5,6, Prop. 7] 参照)

命題　$e>2$ とする。$Aut(\mathcal{S}_m^h)$ は次の例外を除いてすべて一次元の半線形アフィン群 $A\Gamma L_1(q)$ に等しい：$e=3$ で $(m,h)=(1,1),(2,2)$. 例外のときは $\mathcal{S}_1^1 \cong \mathcal{S}_2^2$ であって、$Aut(\mathcal{S}_1^1) \cong 2^3 : SL_3(2)$.

Translation hyperovals の意味付け・特徴付け　平行移動可能な双対超卵型は、ある意味で最も標準的（通常の射影平面中の hyperoval の世界では古典的なものに相当する）であると期待される。従って、次のような問題を考察すべきであろう。

問題　$PG(2d+1,2)$ 中の d-次元の平行移動可能な双対超卵型 $\mathcal{S}_m^h$ を次のいずれかの性質を満たす $PG(2d+1,2)$ 中の d-次元双対超卵型 S として特徴付けできるか？

(i)（幾何学的条件） $PG(2d+1,2)$ の d-次元部分空間 Y でどの $X \in \mathcal{S}_m^h$ に対しても $X \cap Y = \emptyset$ となるものがある。

(ii)（代数的条件） $Aut(S)$ は translation のなす群を含む。（より強い $A\Gamma L_1(q)$ を含む、という仮定から始めてもよい。）

部分空間 $\{(0,y)|y \in GF(1)\}$ は条件 (1) を満たす。この条件 (1) のみによる特徴付けを期待するのは、多少むしがよすぎるかも知れない。というのは $PG(2d,2)$ 中の S_m^{e-m} が条件 (1) と類似の条件によって特徴付けできるとすれば、$PG(2d,2)$ 中の dual hyperoval はすべて translation dual hyperoval と同型になる事になり（「例と分類」での 例 1 の解説を参照)、これは少々強すぎる結果とも思えるからである。ともかく試行錯誤して良い幾何学的特徴付け条件を見いだす必要がある。

一方、条件 (2) のもとで S_m^h が特徴付けできる ($PG(2d,2)$ 中の S_m^{d+1-m} も含めて)、という事は、同様の事実が通常の hyperoval で得られているという事から見て、十分期待して良いかと思われる。

参考文献

[CT] B. Cooperstein and J. Thas, Communication through A. Pasini and A. Del Fra.

[DF] A. Del Fra, On d-dimensional dual hyperovals, preprint, June 12, 1998.

[Hi] J. W. P. Hirschfeldt, *Projective Geometries over Finite Fields*, Oxford Univ. Press, Oxford, 1979.

[HP] C. Huybrechts and A. Pasini, Flag-transitive extensions of dual affine spaces, preprint, 1998.

[Hu] C. Huybrechts, $c.AG^*$-geometries and their consequences for some families of d-dimensional subspaces in $PG(m,q)$, preprint, 1998.

[Ka] W. Kantor, Linear groups containing a Singer cycle, *J. Algebra* **62**, 232–234 (1980).

[Pa] A. Pasini, *Diagram Geometries*, Oxford Univ. Press, Oxford, 1994.

[Th1] J. A. Thas, Projective geometry over a finite field. in: *Handbook of Incidence Geometry, Buildings, and Foundations* (F. Buekenhout, Ed.), Chap.7, pp.295–347, Elsevier Sciences, Amsterdam, 1995.

[Th2] J. A. Thas, Some new classes of extended generalized quadrangles of order $(q+1, q-1)$, to appear in *Proceeding of the Conference at Deinze, 1997.*

[Yo1] S. Yoshiara, A construction of extended generalized quadrangles using the Veronesean, *European J. Combin.* **18** (1997), 835–848.

[Yo2] S. Yoshiara, Extended generalized quadrangles, Report of talk given at Kyoto RIMS on March 9, 1998, for the Conference on Algebraic Combinatorics and related Topics, to appear in *Suriken Kokyuroku* (ed. by A. Munemasa).

[Yo3] S. Yoshiara, A family of d-dimensional dual hyperovals in $PG(2d+1,2)$, preprint, August 4, 1998.

特殊線型群におけるデイド予想

鋤崎 英記 (阪大 理)

1. デイド予想

素数 p に対して、最大正規 p 部分群 $O_p(G)$ が 1 となる有限群 G を考える。p 部分群鎖

$$C : 1 < U_1 < \cdots < U_m$$

を考える。この部分群鎖 C の長さを m とし、$|C|$ で表す。また、1 で始まる G の p 部分群鎖全体を $\mathfrak{P}(G)$ で表す。$g \in G$ に対して、

$$C^g : 1 < U_1^g < \cdots < U_m^g$$

とし、$\mathfrak{P}(G)$ の $G-$ 軌道の完全代表系を $\mathfrak{P}(G)/G$ で表す。C の正規化群を

$$N_G(C) = \{g \in C | C^g = C\} = \bigcap_{j=0}^{m} N_G(P_j)$$

とする。ここで、G の p-block B、負でない整数 d に対して、$N_G(C)$ の複素既約指標 ψ のうち
(i) $|N_G(C)|/\psi(1)$ の p 成分が p^d
(ii) ψ が属する $N_G(C)$ の p-block b が $b^G = B$
を満たすもの全体を $\mathrm{Irr}(H, B, d)$ とする。

以上の記号の下、次のような予想がある。

Conjecture 1 (Dade's ordinary conjecture [D1]). *defect が 0 でない G の p-block B と整数 $d \geq 0$ に対して、*

$$\sum_{C \in \mathfrak{P}(C)/G} (-1)^{|C|} |\mathrm{Irr}(N_G(C), B, d)| = 0$$

が成り立つ。

この予想を強めたものとして、次のようなものがある。

$G \lhd E$ なる群 E をとると、$C \in \mathfrak{P}(G)$ への E の作用が定まる。よって、$N_E(C) = \{g \in E | C^g = C\}$ が定まり、$N_G(C) \lhd N_E(C)$ が成り立つ。これより $\phi \in \mathrm{Irr}(N_G(C))$ への $N_E(C)$ による作用が定まる。ここで、

$$T_{N_E(C)}(\phi) = \{g \in N_E(C) | \phi^g = \phi\}$$

とする。さらに、$\bar{F} \lhd E/G$ に対して、$\phi \in \mathrm{Irr}(N_G(C), B, d)$ のうち
(iii) $GT_{N_E(C)}(\phi)/G = \bar{F}$
を満たすもの全体を $\mathrm{Irr}(N_G(C), B, d, \bar{F})$ とする。このとき、

Conjecture 2 (Dade's invariant conjecture [D2]). *defect が 0 でない G の p-block B と整数 $d \geq 0$、$\bar{F} \lhd E/G$ に対して、*

$$\sum_{C \in \mathfrak{P}(C)/G} (-1)^{|C|} |\mathrm{Irr}(N_G(C). B, d, \bar{F})| = 0$$

が成り立つ。

ここで

$$\mathrm{Irr}(N_G(C),d)=\bigcup_{\text{すべての } p\text{-block } B}\mathrm{Irr}(N_G(C),B,d)$$

とし、Conjecture 1 をすべての pblock について加えると、

(*) $$d>0 \text{ のとき } \sum_{C\in\mathfrak{P}(C)/G}(-1)^{|C|}|\mathrm{Irr}(N_G(C),d)|=0$$

となる。ただし、$d=0$ の場合は defect 0 の p-block に対応するため、和は 0 になるとは限らない。例においては、p-block を無視した (*) を示す。

現在 Dade's conjecture が成り立つ事が示されている群は、散在群の一部など個別の群の他は、$G_2(q)(p\nmid q)$、${}^2G_2(3^{2n+1})(p\neq 3)$、${}^2F_4(2^{2n+1})(p\neq 2)$、$Sz(2^{2n+1})$、$GL(n,q)(p\mid q)$、$S_n$ がある。

(p 部分群鎖について).

部分群鎖の集合として次のようなものを考える。

$\mathfrak{P}(G)$: 1 で始まる G の p-部分群鎖全体

$\mathfrak{E}(G)$: G の初等可換 p-部分群からなる $\mathfrak{P}(G)$ の要素全体

$\mathfrak{N}(G)$: G-部分群鎖 $C:1<U_1<\cdots<U_m$ で、$U_i\lhd U_m$ を満たすもの全体

$\mathfrak{R}(G)$: G-部分群鎖 $C:U_0<U_1<\cdots<U_m$ で、$P_0=O_p(G)$ かつ $P_i=O_p(\bigcap_{j=0}^{i}N_G(P_j))$ $(i=1,2,\cdots,m)$ を満たすもの全体

ここで、$O_p(G)=1$ ならば、$\mathfrak{R}(G)$ は $\mathfrak{P}(G)$ の部分集合である。

Lemma 1 ([KR], [D1]). $O_p(G)=1$ ならば、$\mathfrak{X}$ が $\mathfrak{P}(G)$、$\mathfrak{E}(G)$、$\mathfrak{N}(G)$、$\mathfrak{R}(G)$ のいずれの場合でも

$$\sum_{C\in\mathfrak{X}/G}(-1)^{|C|}|\mathrm{Irr}(N_G(C),B,d,\bar{F})|$$

の値は相等しい。

以下、$\mathfrak{X}=\mathfrak{R}(G)$ で考察を行う。

2. G が CHEVALLEY 群で p が G の定義体の標数と等しい場合

G が Chevalley 群で、p が G の定義体の標数と等しい場合を考える。この時[BT][BW] より、$\mathfrak{R}(G)$ は G の parabolic 部分群の巾単部分群からなる $\mathfrak{P}(G)$ の要素全体である。さらに G の Borel 部分群 U を固定すると、$\mathfrak{R}(G)/G$ は U を含む G の parabolic 部分群の巾単部分群からなる $\mathfrak{P}(G)$ の要素全体である。

U を含む G の parabolic 部分群全体は、G の基本ルート系 I の部分集合全体によりパラメトライズできることが知られている。これにより $J\subseteq I$ に対応するパラボリック部分群を P_J で表す。さらに[W] [KR] により、Conjecture 2 は次と同値である。

Conjecture 3. *defect が 0 でない G の p-block B と整数 $d\geq 0$、$\bar{F}\lhd E/G$ に対して、*

$$\sum_{J\subseteq I}(-1)^{|I\setminus J|}|\mathrm{Irr}(P_J,B,d,\bar{F})|=0$$

が成り立つ。

例 1. $G=G_2(q)$, $q=2^f$, $p=2$ の場合

[EY] により、$G_2(q)$ とそのパラボリック部分群の既約指標が求められている。$G_2(q)$ の基本ルート系を $I=\{a,b\}$ とすると、パラボリック部分群は $P_\emptyset=U$, $P_{\{a\}}$, $P_{\{b\}}$, $P_I=G_2(q)$ の 4 つである。このとき、$|\mathrm{Irr}(P_J,d)|$ は次の表の通りになり、(*) が成り立つことが分かる。

	$d=6f$	$d=5f+1$	$d=5f$	$d=4f$	$d=3f$	$d=0$
$J=\emptyset$	q^2	4	$4q-3+gcd(q-1,3)^2$	q		
$J=\{a\}$	q^2	4	$2q+2$	q	1	
$J=\{b\}$	q^2	4	$4q-3+gcd(q-1,3)^2$			
$J=I$	q^2	4	$2q+2$		1	1

3. $G = SL(n,q)$, $p|q$ の場合の DADE'S CONJECTURE

G が特殊線型群 $SL(n,q)$, $q=p^f$ の場合を考える。

基本ルート系を $I=\{1,2,\cdots,n-1\}$ とし、Borel 部分群 U として下三角行列からなる群をとる。このとき、$J\subseteq I$ が $I\backslash J=\{a_1,\cdots,a_k\}$ であれば、

$$P_J=\{(p_{ij})\in SL(n,q)|\ \text{ある } k \text{ について } i\le a_k \text{ または } j>a_k \text{ ならば } p_{ij}=0\}$$

例 2. $n=3$ の場合、$I=\{1,2\}$ とすると、$P_\emptyset=\left\{\begin{pmatrix}*&0&0\\*&*&0\\*&*&*\end{pmatrix}\right\}$, $P_{\{1\}}=\left\{\begin{pmatrix}*&*&0\\*&*&0\\*&*&*\end{pmatrix}\right\}$, $P_{\{2\}}=\left\{\begin{pmatrix}*&0&0\\*&*&*\\*&*&*\end{pmatrix}\right\}$, $P_I=SL(3,q)$ となる。

このとき、$|\mathrm{Irr}(P_J,d)|$ は次の表の通りになり、(*) が成り立つことが分かる。

	$d=3f$	$d=2f$	$d=0$
$J=\emptyset$	$q^2-1+gcd(q-1,3)^2$	$q-1$	
$J=\{1\}$	$q^2-1+gcd(q-1,3)^2$	$q-1$	
$J=\{2\}$	$q^2-1+gcd(q-1,3)^2$	$q-1$	
$J=I$	$q^2-1+gcd(q-1,3)^2$	$q-1$	1

さらに一般の n に対しては、$E=GL(n,q)$ の場合の Dade's invariant conjecture が成り立つ。すなわち、

Theorem[S2]. *$G=SL(n,q)$, $p|q$, $E=GL(n,q)$ とすると、Conjecture 3 が成り立つ。*

ここで、$SL(n,q)$ の princial block は中心への制限が自明な指標の和となる次数 $n(n-1)/2$ 未満の既約指標全体である[S1]。これは $PSL(n,q)$ の defect 0 でない唯一の p-block と同一視できる。このことよりただちに次のことが言える。

Corollary[S2]. *$G=PSL(n,q)$, $p|q$, $E=PGL(n,q)$ とすると、Conjecture 3 が成り立つ。*

Theorem の証明は次のようにおこなった。

(1)$GL(n,q)/SL(n,q)$ が巡回群であるから、その部分群は位数で決定できる。このことと Clifford の定理を用いて、$SL(n,q)$ の指標の固定化群に関する命題を、$GL(n,q)$ の指標の $SL(n,q)$ への制限による既約成分の個数に関する命題に言い換えることができる。すなわち、$G'=GL(n,q)$ の parabolic 部分群 P'_J に対し、$\mathrm{Irr}(P'_J,B,d)$ の要素で $P'_J\cap SL(n,q)$ 制限による既約成分の数が s であるもの全体を $\mathrm{Irr}'(P'_J,B,d,s)$ とすると、Conjecture 3 は次と同値である。「G' の自明でない defect 群を持つ p-block B と $d,s\ge 0$ に対して、

$$\sum_{J\subseteq I}(-1)^{|I\backslash J|}|\mathrm{Irr}'(P'_J,B,d,s)|=0$$

が成り立つ」

(2)$GL(n,q)$ については Conjecture 1 が成り立つことが証明されている[OU]。この証明を[L][S] と Mackey 分解を用いて $P'_J\cap SL(n,q)$ 制限まで考慮に入れた形に拡張した。具体的には、P'_J をいくつかの一般線型群の parabolic 部分群の直積と適当な可換正規部分群との半直積で表し、低い次数の問題に帰納することにより証明した。

References

[BT] A. Borel and J. Tits: *Eléments unipotents et sous-groupes paraboliques des groupes réductifs, I*, Invent. Math. 12 (1971), 95–104.

[BW] N. Burgoyne and C. Williamson: *On a theorem of Borel and Tits for finite Chevalley groups*, Arch. Math. 27 (1976), 489–491.

[D1] E. C. Dade: *Counting characters in blocks, I*, Invent. Math. 109 (1992), 187–210.

[D2] E. C. Dade: *Counting characters in blocks, 2.9*, Representation Theory of Finite Groups (R. Solomon, ed.), Walter de Gruyter & Co., Berlin · New York, 1997, p. 45–59.

[EY] H. Enomoto and H. Yamada: *The characters of* $G_2(2^n)$, Japan. J. Math. 12 (1986), 325–377.

[KR] R. Knörr and G. Robinson: *Some remarks on a conjecture of Alperin*, J. London Math. Soc. (2)39 (1989), 48–60.

[L] G. I. Lehrer:, *Characters, Classes, and Duality in Isogenous Groups*, J. Algebra 36 (1975), 278–286.

[OU] J. B. Olsson and K. Uno: *Dade's conjecture for general linear groups in the defining characteristic*, Proc. London Math. Soc. (3)72 (1996), 359–384.

[S1] H. Sukizaki: *The Mckay numbers of a subgroup of* $GL(n,q)$ *containing* $SL(n,q)$, Osaka J. Math. (accepted).

[S2] H. Sukizaki: *Dade's conjecture for special linear groups in the defining characteristic* (in preparation).

[W] P. J. Webb *Subgroup complexes*, The Arcara conference on Representaions of Finite Groups (Proceeding of Symposia in Pure Mathematics 47 (American Mathematical Society, Providence, R. I. 1987)) (P. Fong, ed.), p. 349–365.

二面体群の普遍R行列と結び目の不変量

阪大・理　和久井道久

このノートでは、以下の非可換な有限群について、その複素数体 $\mathbf{C}$ 上の群環の普遍R行列を決定する。

・位数 $2m$ の二面体群 D_{2m} $(m \geq 3)$ ： $D_{2m} =< s,\ t \mid s^m = 1,\ t^2 = 1,\ t^{-1}st = s^{-1} >$

・位数 $4n$ の一般四元数群 Q_{4n} $(n \geq 2)$ ： $Q_{4n} =< s,\ t \mid s^{2n} = 1,\ t^2 = s^n,\ t^{-1}st = s^{-1} >$

・位数 $8p$ の準二面体群 SD_{8p} $(p \geq 3)$ ： $SD_{8p} =< s,\ t \mid s^{4p} = 1,\ t^2 = 1,\ t^{-1}st = s^{2p-1} >$

・次の表示を持つ位数 $8p$ $(p \geq 3)$ の群： $SA_{8p} :=< s,\ t \mid s^{4p} = 1,\ t^2 = 1,\ t^{-1}st = s^{2p+1} >$

・位数 m の巡回群と位数 2 の巡回群の wreath 積 W_{2m^2} $(m \geq 3)$ ：

$$W_{2m^2} =< s_1, s_2, t \mid s_1^m = s_2^m = 1,\ t^2 = 1,\ s_1s_2 = s_2s_1,\ ts_1t^{-1} = s_2 >$$

・4次交代群 A_4 ：

$$A_4 =< s_1, s_2, t \mid s_1^2 = s_2^2 = 1,\ t^3 = 1,\ s_1s_2 = s_2s_1,\ ts_1 = s_2t,\ ts_1s_2 = s_1t >$$

普遍R行列の概念はDrinfel'd [3]により与えられた。Drinfel'd[3]とJimbo[5]は「量子群」と呼ばれる無限次元の非可換非余可換ホップ代数を定義したが、Drinfel'd は、さらに、量子群には準三角ホップ代数の構造が「入る」ことを見い出し、具体的に普遍R行列を構成して見せた。それ以来、多くの研究者によって準三角ホップ代数の理論や例が研究され、他の分野にその理論が応用されている。準三角ホップ代数や普遍R行列の定義を思い出しておこう[3][4]。

定義(Drinfel'd)　$A = (A, \Delta, \varepsilon, S)$ をホップ代数 とし、$R \in A \otimes A$ を可逆元とする。組 (A, R) が準三角ホップ代数であるとは、次の3つの条件が満たされるときをいう：

(i) $\Delta'(a) = R \cdot \Delta(a) \cdot R^{-1}$　for all $a \in A$

(ii) $(\Delta \otimes id)(R) = R_{13}R_{23}$

(iii) $(id \otimes \Delta)(R) = R_{13}R_{12}$

ここで、$\Delta' = T \circ \Delta$, $T : A \otimes A \longrightarrow A \otimes A$, $T(a \otimes b) = b \otimes a$ であり、$R_{ij} \in A \otimes A \otimes A$ は $R_{12} = R \otimes 1$, $R_{23} = 1 \otimes R$, $R_{13} = (T \otimes id)(R_{23})$ で与えられる。R を普遍R行列と呼ぶ。

有限群 G に対して、その群環 $\mathbf{C}[G]$ は

$$\Delta(g) = g \otimes g, \quad \varepsilon(g) = 1, \quad S(g) = g^{-1}, \quad g \in G$$

によってホップ代数になる。群環 $\mathbf{C}[G]$ の普遍R行列を有限群 G の普遍R行列と呼ぶことにする。1 を有限群 G の単位元とするとき、明らかに、$R = 1 \otimes 1$ は G の普遍R行列である。

普遍R行列があると、どのようないいことがあるのだろうか。いろいろな答えがあると思うが、ここでは、低次元多様体論への応用という観点から述べてみたい。

まず、ホップ代数 A の2つの表現に対して、テンソル積表現が定義されることに注意しよう。V,W を左 A-加群とする。このとき、ベクトル空間としてのテンソル積 $V\otimes W$ への A の作用を

$$a\cdot v\otimes w=\sum_i a_i\cdot v\otimes a_i'\cdot w,\quad a\in A,v\in V,w\in W,\quad \Delta(a)=\sum_i a_i\otimes a_i'$$

と定める。Δ が代数準同型であることから、この作用は $V\otimes W$ に左 A-加群の構造を与えていることがわかる。

一般に、$V\otimes W$ と $W\otimes V$ の間のベクトル空間としての標準的な同型 $v\otimes w\longmapsto w\otimes v$ は A の作用を保たない。A に普遍R行列 R が存在すれば、$V\otimes W$ と $W\otimes V$ の間の表現としての同型を作ることができる。実際、

$$\check{R}_{V,W}(v\otimes w)=\sum_i \beta_i\cdot w\otimes \alpha_i\cdot v,\quad v\in V,w\in W,\ R=\sum_i \alpha_i\otimes\beta_i$$

によって定義される写像 $\check{R}_{V,W}$ は準三角ホップ代数の条件 (i) により、表現としての同型を与えることがわかる。

普遍R行列を考える上で大切なことは、準三角ホップ代数の表現 V を与えるごとに、n 次組み紐群 B_n の表現 $F:B_n\longrightarrow GL(V^{\otimes n})$ が次のようにして得られるということである。

$F($  $)=id_V\otimes\cdots\otimes id_V\otimes\check{R}_{V,V}\otimes id_V\otimes\cdots\otimes id_V$

実際、準三角ホップ代数の条件 (i)(ii) から

$$(\check{R}_{V,V}\otimes id_V)(id_V\otimes\check{R}_{V,V})(\check{R}_{V,V}\otimes id_V)=(id_V\otimes\check{R}_{V,V})(\check{R}_{V,V}\otimes id_V)(id_V\otimes\check{R}_{V,V})$$

が成り立つので、F は B_n の表現を与えることがわかる。

今述べた B_n の表現 F を使って、絡み目の不変量を構成する方法を簡単に説明しよう。絡み目とは、有限個の円周の3次元球面 S^3 または3次次元ユークリッド空間 $\mathbf{R}^3$ への埋め込みのことをいう。S^3 または $\mathbf{R}^3$ の ambient isotopy でうつりあう2つの絡み目は同じ絡み目とみなす。組み紐 b の端点を図1のように張り合わせることにより、絡み目 $b^\wedge$ を得ることができる。$b^\wedge$ を b の閉包と呼ぶ。Alexander によって、任意の絡み目はある組み紐の閉包として得られることがわかっている。つまり、次の可換図式の上段の写像は全射である。この写像は単射ではない。実際、図2の2つの組み紐の閉包は同じ絡み目を与えることが容易にわかる。実は、2つの組み紐の閉包が同じ絡み目を与えるための必要十分条件は、その2つの組み紐が、組み紐関係式(図3)および図2の2つの組み紐が同値であるという関係式の有限列で関係づけられることであることが知られている(Markov の定理)。

$$\begin{array}{ccc}\bigcup_{n\geq 1} B_n & \xrightarrow{\text{閉包をとる}} & \{\text{the links}\}\\ \Big\downarrow F & & \Big\downarrow F\\ \bigcup_{n\geq 1} GL(V^{\otimes n}) & \xrightarrow{\text{Trace}} & \mathbf{C}\end{array}$$

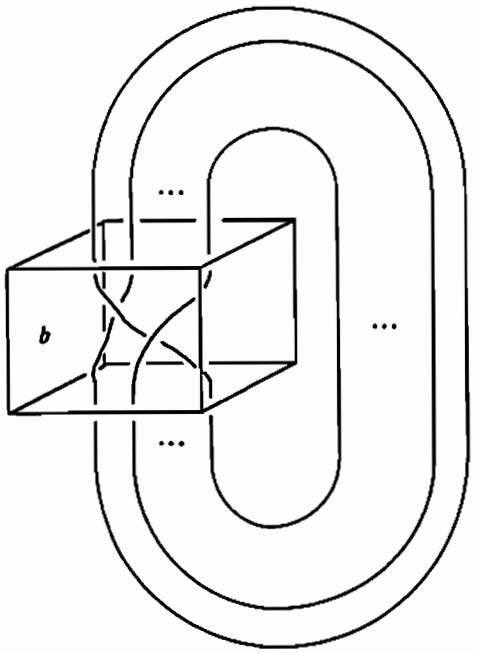


図 1

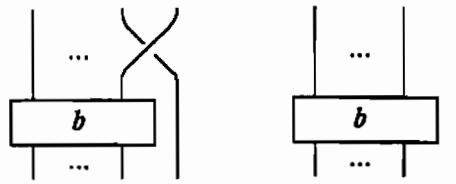


図 2

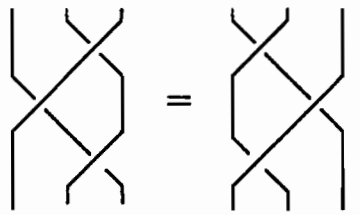
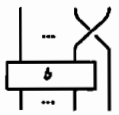
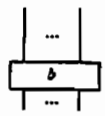


図 3

ところで、準三角ホップ代数の表現 V が与えられると、先ほどのようにして、組み紐群 B_n の表現 F が得られる。したがって、写像 $F : \cup_n B_n \longrightarrow \cup_n GL(V^{\otimes n})$ が得られる。V が有限次元ならば、$V^{\otimes n}$ 上の線形変換に対してはトレースをとるという操作が可能である。(線形変換に対してトレースをとるという操作と組み紐に対して閉包をとるという操作は「同じ」と思うことができる。ここで、「同じ」といったのは、どちらもある種のモノイダル圏におけるトレースとして実現されるという意味である。)もし、

Trace$F$() と Trace$F$() が一致するならば、

上の図式を可換にする写像 $\bar{F}$: {the links} $\longrightarrow$ C が導かれて、絡み目の不変量が得られる。しかしながら、一般に、上の 2 つは等しくない。Reshetikhin と Turaev [10]は、準三角ホップ代数にさらにリボン元と呼ばれるよい性質を持った元が存在するならば、V を有限次元既約表現にとり、トレースを若干修正することにより、図式を可換にする絡み目の不変量 $\bar{F}$ が得られることを示した[†]。

こうした方法で定義される絡み目の不変量としては、次の2つのものがよく研究されている。1つは、量子群の表現を使って定義される、いわゆる量子不変量である。この不変量の族は、Alexsander 多項式や Jones 多項式などのよく知られた多項式不変量を豊富に含んでいる。もう1つは、有限群の群環のなすホップ代数を量子二重構成[3]することにより得られる準三角ホップ代数から定義される不変量である。この準三角ホップ代数から作られる絡み目の不変量は、絡み目の補空間の基本群のその有限群への準同型写像の個数である。

「もう少し別の種類の」準三角ホップ代数を使って、興味深い不変量を導くことができないだろうか。有限群の群環のなすホップ代数に(非自明な)普遍R行列の解を見つけて、Reshetikhin-Turaev の方法で不変量を構成したらどのような不変量が得られるだろうか。これに関しては、H.Murakami, Ohtsuki, Okada[7]による仕事がある。彼らは、枠付き絡み目の絡み行列を用いて3次元多様体の不変量を構成したが、この不変量は、本質的に、巡回群の群環の普遍R行列から構成される Reshetikhin-Turaev 型の不変量である(上では説明しなかったが、準三角ホップ代数とその表現の有限個の族がある種の条件を満たすと、それらの表現の族に関して絡み目の不変量の和をとることにより、3次元多様体の不変量が定義される[11])。この不変量はまた、Dijkgraaf-Witten 不変量や牛腸不変量などの3次元多様体の不変量やDate, Jimbo, Miki, Miwa によって定義された絡み目の cyclotomic 不変量と密接に関係していることでも興味深い。

では、非可換な有限群の普遍R行列から Reshetikhin-Turaev 型の不変量を構成したら、もっと面白い不変量が得られるのではないだろうか。最初は、どうやって普遍R行列を求めたらよいのかわからなかったが、川中先生からの助言もあって、位数 8 の二面体群 D_8 、位数 8 の一般四元数群 Q_8、位数 $8p$ $(p \geq 3)$ の準二面体群 SD_{8p}、位数 $8p$ $(p \geq 3)$ の群 SA_{8p} に新しい普遍R行列の例を見つけることができた。残念なことに、それらの新しい普遍R行列は、Reshetikhin-Turaev 型の3次元多様体の不変量を構成するのに必要な条件を満たしていないことがわかった。また、Reshetikhin と Turaev の方法で定義される絡み目の不変量については、どのような絡み目についても同じ値をとる、つまらない不変量であることもわかった。

今のところ、有限群の群環でつくられる準三角ホップ代数の場合、巡回群（あるいは、それらの直和で得られるアーベル群）から構成される不変量を越えるような面白い不変量は得られていない。もちろん、すべての有限群について調べ挙げたわけではないので、まだ、その中に興味深いもの残されている可能性は否定できない。

§.1 主定理

まず、巡回群の普遍R行列に関して知られている結果を引用する。

補題1 (H.Murakami-Ohtsuki-Okada[7]、Radford[8][9]) $\mathbf{Z}_m$ を位数 m の巡回群とする。このとき、$\mathbf{Z}_m$ の普遍R行列は全部で m 個ある。s をその生成元とし、ζ を 1 の原始 m 乗根とするとき、それらは

$$R = \frac{1}{m} \sum_{k,i=0}^{m-1} \zeta^{-ik} s^k \otimes s^{di}$$

で与えられる。ここで、$d \in \{0, 1, \cdots, m-1\}$ である。以下、この普遍R行列を R_d として引用する。□

m は 3 以上の整数、n は 1 以上の整数、q は $1 \leq q \leq m-1$ を満たす整数であるとし、2

つの元で生成される有限群

$$D_{m,n,q} =< s,\ t \mid s^m = 1,\ t^2 = s^n,\ t^{-1}st = s^q >$$

を考える。$D_{m,n,q}$ は $m = n$ かつ $q = 1$ のとき、位数 m の巡回群と位数 2 の巡回群との直和であり、$m = n$ かつ $q = m - 1$ のとき位数 $2m$ の二面体群であり、$m = 2n$ かつ $q = m - 1$ のとき位数 $4n$ の一般四元数群であり、$m = n = 4p$ かつ $q = 2p - 1$ のとき位数 $8p$ の準二面体群 SD_{8p} であり、$m = n = 4p$ かつ $q = 2p + 1$ のとき位数 $8p$ の群 SA_{8p} である。

$D_{m,n,q}$ の位数が $2m$ であるとき、s で生成される $D_{m,n,q}$ の部分群 $< s >$ は位数 m の巡回群であるので、これを $\mathbf{Z}_m$ と同一視して $\mathbf{Z}_m$ を $D_{m,n,q}$ の部分群とみなす。

m, q が条件「各 $k \in \{0, 1, \cdots, m-1\}$ に対して $qj \equiv k \pmod{m}$ となる $j \in \{0, 1, \cdots, m-1\}$ が唯一存在する」を満たしているとする。このとき、各 k に対して定まる j を $\sigma(k)$ と書くことにする：

$$q\sigma(k) \equiv k \mod m. \tag{1.1}$$

もし、任意の $i, k \in \{0, 1, \cdots, m-1\}$ について

$$\sigma(i)\sigma(k) = ik \tag{1.2}$$

が成り立っているならば、R_d $(d = 0, 1, \cdots, m-1)$ は $\Delta'(t) \cdot R_d = R_d \cdot \Delta(t)$ を満たすので、$\mathbf{C}[D_{m,n,q}]$ の普遍R行列になる。$q = m - 1$ の場合、$m = n = 4p$ かつ $q = 2p \pm 1$（但し、$p \geq 3$）の場合のいずれの場合も条件(1.2)を満たすので、R_d は $\mathbf{C}[D_{m,n,q}]$ の普遍R行列になる。実は次が成立する。

定理 2

(i) 群 $D_{m,n,m-1}$ $(m \geq 3,\ n \geq 1)$ が R_d $(d = 0, 1, \cdots, m-1)$ 以外の普遍R行列を持つのは、$m = 4$ かつ n が偶数のときに限る。$m = 4$ かつ n が偶数のとき、R_d $(d = 0, 1, \cdots, m-1)$ 以外の普遍R行列は次の式で与えられる 4 つである。

$$\tilde{R}_{a,\mu} = \frac{1}{4} \sum_{\alpha,\beta,i,j=0,1} a^{\alpha\beta} (-1)^{\alpha\beta\mu + j\alpha + i\beta} t^{\alpha} s^{2i+\alpha\mu} \otimes t^{\beta} s^{2j+\beta\mu}$$

但し、$a^2 = (-1)^{\frac{n}{2}}$, $\mu = 0, 1$ である。

(ii) 群 $D_{4p,4p,2p-1}$ $(p \geq 3)$ は R_d $(d = 0, 1, \cdots, m-1)$ 以外の普遍R行列を $4p$ 個持つ。それらは次の式で与えられる。

$$\tilde{R}_c = \frac{1}{4} \sum_{\alpha,\beta,\gamma,\delta=0,1} a^{\alpha\beta} (-1)^{\beta\gamma + \alpha\delta} \zeta^{-2c\alpha\beta} t^{\alpha} s^{c\alpha + 2p\gamma} \otimes t^{\beta} s^{c\beta + 2p\delta}$$

但し、$c = 0, 1, \cdots, 2p-1$ であり、ζ は 1 の原始 $4p$ 乗根であり、$a^2 = (-1)^c \zeta^{4c}$ である。

(iii) 群 $D_{4p,4p,2p+1}$ $(p \geq 3)$ は R_d $(d = 0, 1, \cdots, m-1)$ 以外の普遍R行列を $4p$ 個持つ。それらは次の式で与えられる。

$$\tilde{R}_c = \frac{1}{16p^2} \sum_{\substack{\alpha,\beta=0,1 \\ i,j=0,1,\cdots,4p-1}} a^{\alpha\beta} \zeta^{j\alpha + i\beta} \sum_{k,l=1,\cdots,2p} \zeta^{-2(ki+lj) + 2c(2kl - k\alpha - l\beta)} t^{\alpha} s^{i} \otimes t^{\beta} s^{j}$$

但し、$c=0,1,\cdots,2p-1$ であり、ζ は 1 の原始 $4p$ 乗根であり、$a^2=(-1)^c\zeta^{2c}$ である。

定理 2 は次の節で証明される。次に、$\mathbf{Z}_m$ と $\mathbf{Z}_2$ との wreath 積 W_{2m^2} と 4 次交代群 A_4 の普遍R行列に関する結果を述べるために、補題を 1 つ引用する。

補題 3 (Radford[8]) $\mathbf{Z}_m$ を位数 m の巡回群とする。このとき、$\mathbf{Z}_m\oplus\mathbf{Z}_m$ の普遍R行列は全部で m^4 個ある。s_1,s_2 をその生成元とし、ζ を 1 の原始 m 乗根とするとき、それらは

$$R=\frac{1}{m^2}\sum_{i,j,k,l=0}^{m-1}\zeta^{-(ij+kl)}s_1^is_2^k\otimes s_1^{pj+rl}s_2^{qj+sl}$$

で与えられる。ここで、$p,q,r,s\in\{0,1,\cdots,m-1\}$ である。以下、この普遍R行列を R_{pqrs} として引用する。□

wreath 積 W_{2m^2} $(m\geq 3)$ の s_1,s_2 で生成される部分群を $\mathbf{Z}_m\oplus\mathbf{Z}_m$ と同一視するとき、

$$\Delta'(t)\cdot R_{pqrs}=R_{srqp}\cdot\Delta(t)$$

が成立する。従って、R_{pqqp} $(p,q\in\{0,1,\cdots,m-1\})$ は W_{2m^2} の普遍R行列である。

また、4 次交代群 A_4 の s_1,s_2 で生成される部分群を $\mathbf{Z}_2\oplus\mathbf{Z}_2$ と同一視するとき、$\mathbf{Z}_2\oplus\mathbf{Z}_2$ の16 個の普遍R行列のうち、$\Delta'(t)\cdot R_{pqrs}=R_{pqrs}\cdot\Delta(t)$ を満たすものは、$R_{0000}=1\otimes 1, R_{0110}, R_{1011}, R_{1101}$ の 4 個のみである。

定理 4

(i) $\mathbf{Z}_m$ と $\mathbf{Z}_2$ の wreath 積 W_{2m^2} $(m\geq 3)$ の普遍R行列は全部で m^2 個あり、それらは、s_1,s_2 で生成される巡回群の直和の普遍R行列の中の R_{pqqp} $(p,q\in\{0,1,\cdots,m-1\})$ である。

(ii) 4 次交代群 A_4 の普遍R行列は全部で 4 個あり、それらは、s_1,s_2 で生成される巡回群の直和の普遍R行列の中の $R_{0000}=1\otimes 1, R_{0110}, R_{1011}, R_{1101}$ である。

定理 4 は定理 2 と同様の方法で証明される††。

§.2 定理 2 の証明

最初に、このノートで用いる基本的な補題を 2 つ用意しておく。最初の補題は準三角ホップ代数の定義からただちに得られる。2 番目の補題は Rodford [8] によって指摘された。

補題 5 組 (A,R) が準三角ホップ代数ならば、$(\varepsilon\otimes id)(R)=1$, $(id\otimes\varepsilon)(R)=1$ が成り立つ。□

補題 6 ([8, p.4 Lemma1]) A をホップ代数とする。このとき、$R\in A\otimes A$ が

(i) $(\Delta\otimes id)(R)=R_{13}R_{23}$

(ii) $(\varepsilon\otimes id)(R)=1$

を満たしているならば、R は可逆である。□

一般に、有限群 G の $\mathbf{C}$ 上の既約指標の全体を $\chi_1,\cdots,\chi_n$ とするとき、各 $i=1,\cdots,n$ に対して

$$E_i := \frac{\deg\chi_i}{|G|}\sum_{g\in G}\chi_i(g^{-1})g \quad \in \mathbf{C}[G]$$

とおくと、E_i $(i=1,\cdots,n)$ は $\mathbf{C}[G]$ の原始べき等元である。すなわち、

$$E_iE_j=\delta_{ij}E_i \quad (i,j=1,\cdots,n), \quad E_1+\cdots+E_n=1$$

が成立する。

$\mathbf{Z}_m$ を位数 m の巡回群とし、その生成元を s とする。ζ を 1 の原始 m 乗根とする。$\mathbf{Z}_m$ の既約指標 χ_k $(k=0,1,\cdots,m-1)$ は

$$\chi_k(s^i)=\zeta^{ki} \quad (i=0,1,\cdots,m-1)$$

で与えられる。χ_k $(k=0,1,\cdots,m-1)$ に対応する原始べき等元 E_k は

$$E_k=\frac{1}{m}\sum_{i=0}^{m-1}\zeta^{-ki}s^i \tag{2.1}$$

である。$E_ks=\zeta^kE_k$ となるから、$i=0,1,\cdots,m-1$ に対して

$$s^i=1\cdot s^i=\sum_{k=0}^{m-1}E_ks^i=\sum_{k=0}^{m-1}\zeta^{ik}E_k$$

が成立する。便宜上、任意の整数 k に対して E_k を(2.1)の右辺によって定義すれば、$E_{m+k}=E_k$ $(k\in\mathbf{Z})$ が成り立つ。ζ は 1 の原始 m 乗根であるので、任意の整数 p に対して

$$\sum_{i=0}^{m-1}\zeta^{ip}=\begin{cases} m & \text{if } p\equiv 0 \bmod m \\ 0 & \text{otherwise}\end{cases}$$

となる。このことに注意すると、$\Delta(E_k)=\sum_{j=0}^{m-1}E_j\otimes E_{k-j}$ を得る。

(定理 2 の証明) m は 3 以上の整数、n は 1 以上の整数、q は $2\le q\le m-1$ を満たす整数であるとする。$D_{m,n,q}$ の位数は $2m$ であるとする。s で生成される $D_{m,n,q}$ の部分群 $<s>$ は位数 m の巡回群であるので、これを $\mathbf{Z}_m$ と同一視して $\mathbf{Z}_m$ を $D_{m,n,q}$ の部分群とみなす。このとき、先程求めた $\mathbf{Z}_m$ の原始べき等元 $E_0,E_1,\cdots,E_{m-1}$ に $tE_0,tE_1,\cdots,tE_{m-1}$ を加えて得られる $2m$ 個の $\mathbf{C}[D_{m,n,q}]$ の元は $\mathbf{C}[D_{m,n,q}]$ の基底をなす。我々はこの基底を使って $q=m-1$ の場合、$m=n=4p$ かつ $q=2p\pm1$ の場合に $D_{m,n,q}$ の普遍R行列を決定する。

まず、$D_{m,n,q}$ の関係式から

$$s^it=ts^{iq} \quad \text{for } \forall i\in\mathbf{Z}$$

が導かれることに注意する。

各 $k \in \{0,1,\cdots,m-1\}$ に対して $qj \equiv k \mod m$ を満たす $j \in \{0,1,\cdots,m-1\}$ が唯一存在すると仮定する。この j を $\sigma(k)$ と書く。すると、$k \in \{0,1,\cdots,m-1\}$ に対して

$$E_k s = \zeta^k E_k, \qquad E_k t = t E_{\sigma(k)}$$

となる。

$R \in \mathrm{C}[D_{m,n,q}] \otimes \mathrm{C}[D_{m,n,q}]$ を $D_{m,n,q}$ の普遍R行列とし、

$$R = \sum_{\substack{\alpha,\beta=0,1 \\ i,j=0,1,\cdots,m-1}} a_{\beta j}^{\alpha i}\, t^\alpha E_i \otimes t^\beta E_j \quad (a_{\beta j}^{\alpha i} \in \mathrm{C})$$

と書く。

$$R \cdot s \otimes s = \sum_{\substack{\alpha,\beta \\ i,j}} a_{\beta j}^{\alpha i} \zeta^{i+j} t^\alpha E_i \otimes t^\beta E_j,$$

$$s \otimes s \cdot R = \sum_{\substack{\alpha,\beta \\ i,j}} a_{\beta j}^{\alpha i} t^\alpha s^{q^\alpha} E_i \otimes t^\beta s^{q^\beta} E_j = \sum_{\substack{\alpha,\beta \\ i,j}} a_{\beta j}^{\alpha i} \zeta^{q^\alpha i + q^\beta j} t^\alpha E_i \otimes t^\beta E_j$$

より

$$s \otimes s \cdot R = R \cdot s \otimes s \iff a_{\beta j}^{\alpha i} \zeta^{i+j} = a_{\beta j}^{\alpha i} \zeta^{q^\alpha i + q^\beta j} \quad \text{for all } \alpha,\beta,i,j \quad \cdots\cdots(\textbf{1})$$

となる。特に、

$$a_{0j}^{1i} = a_{11}^{0i} = 0 \quad \text{for } i,j = 0,1,\cdots,m-1 \quad \cdots\cdots(\textbf{2})$$

となることがわかる($2 \le q \le m-1$ に注意)。次に、$E_k t = t E_{\sigma(k)}$ $(k = 0,1,\cdots,m-1)$ となることから

$$t \otimes t \cdot R = R \cdot t \otimes t \iff a_{\beta j}^{\alpha i} = a_{\beta\ \sigma(j)}^{\alpha\ \sigma(i)} \quad \text{for all } \alpha,\beta,i,j \quad \cdots\cdots(\textbf{3})$$

が得られる。以下、$a_{\beta j}^{\alpha i}$ の添字 i,j は m を法として考えることにする。

$$(\Delta \otimes id)(R) = \sum_{\substack{\alpha,\beta \\ i,j}} \sum_{k} a_{\beta j}^{\alpha i}\, t^\alpha E_k \otimes t^\alpha E_{i-k} \otimes t^\beta E_j,$$

$$R_{13} R_{23} = \sum_{\substack{\alpha,\beta,\alpha',\beta' \\ i,j,k,l}} a_{\beta l}^{\alpha k} a_{\beta' j}^{\alpha' i}\, t^\alpha E_k \otimes t^{\alpha'} E_i \otimes t^{\beta+\beta'} E_{\sigma^{\beta'}(l)} E_j$$

$$= \sum_{\substack{\alpha,\alpha',\beta \\ i,j,k}} \sum_{\beta_1+\beta_2=\beta} a_{\beta_1 \sigma^{-\beta_2}(j)}^{\alpha\ \ k} a_{\beta_2 j}^{\alpha' i} \zeta^{nj\beta_1\beta_2}\, t^\alpha E_k \otimes t^{\alpha'} E_i \otimes t^\beta E_j$$

となる。したがって、$(\Delta \otimes id)(R) = R_{13} R_{23}$ となるための必要十分条件は任意の $\alpha,\alpha',\beta = 0,1$, $i,j,k = 0,1,\cdots,m-1$ に対して

$$\delta_{\alpha,\alpha'} a_{\beta\ j}^{\alpha\ i+k} = \sum_{\beta_1+\beta_2=\beta} a_{\beta_1 \sigma^{-\beta_2}(j)}^{\alpha\ \ k} a_{\beta_2 j}^{\alpha' i} \zeta^{nj\beta_1\beta_2} \quad \cdots\cdots(\textbf{4})$$

となることである。ここで、$\delta_{\alpha,\alpha'}$ はクロネッカーのデルタである。同様にして、$(id\otimes\Delta)(R)=R_{13}R_{12}$ となるための必要十分条件は任意の $\alpha,\beta,\beta'=0,1,\ i,j,k=0,1,\cdots,m-1$ に対して

$$\delta_{\beta,\beta'}a_{\beta\ k+j}^{\alpha\ i}=\sum_{\alpha_1+\alpha_2=\alpha}a_{\beta\ \ k}^{\alpha_1\sigma^{-\alpha_2}(i)}a_{\beta'j}^{\alpha_2 i}\zeta^{ni\alpha_1\alpha_2}\qquad\cdots\cdots(❹')$$

となることである。(❹)(❹′)を繰り返し用いて

$(\Delta\otimes id)(R)=R_{13}R_{23}$

$\Longrightarrow$ 任意の $\alpha,\beta=0,1,\ i,j=0,1,\cdots,m-1$ に対して

$$a_{\beta\ j}^{\alpha\ i+1}=\sum_{\beta_1+\beta_2+\cdots+\beta_{i+1}=\beta}\Big(\prod_{g=1}^{i}a_{\beta_g\ \sigma^{-\beta_{g+1}-\cdots-\beta_{i+1}}(j)}^{\alpha\quad 1}\Big)a_{\beta_{i+1}j}^{\alpha\quad 1}\zeta^{nj\sum_{u<v}\beta_u\beta_v},\tag{2.2}$$

$(id\otimes\Delta)(R)=R_{13}R_{12}$

$\Longrightarrow$ 任意の $\alpha,\beta=0,1,\ i,j=0,1,\cdots,m-1$ に対して

$$a_{\beta\ 1+j}^{\alpha\ i}=\sum_{\alpha_1+\alpha_2+\cdots+\alpha_{j+1}=\alpha}\Big(\prod_{g=1}^{j}a_{\beta\quad 1}^{\alpha_g\ \sigma^{-\alpha_{g+1}-\cdots-\alpha_{j+1}}(i)}\Big)a_{\beta\quad 1}^{\alpha_{j+1}i}\zeta^{ni\sum_{u<v}\alpha_u\alpha_v}\tag{2.3}$$

を得る。ここで、(❷)を使うと

$$\begin{cases}a_{\beta\ j}^{1\ i+1}= & \delta_{\beta,i+1}\Big(\prod_{g=0}^{i}a_{1\ \sigma^{-g}(j)}^{1\ 1}\Big)\zeta^{nj\frac{i(i+1)}{2}},\\ a_{1\ 1+j}^{\alpha\ i}= & \delta_{\alpha,j+1}\Big(\prod_{g=0}^{j}a_{1\ 1}^{1\ \sigma^{-g}(i)}\Big)\zeta^{ni\frac{j(j+1)}{2}}\end{cases}\tag{2.4}$$

となることがわかる。但し、$\delta_{\beta,i+1}$, $\delta_{\alpha,j+1}$ は 2 を法としたクロネッカーのデルタである。よって、$i,j=0,1,\cdots,m-1$ に対して、

$$\begin{cases}a_{0\ j}^{1\ i}=0 & \text{if } i \text{ is odd},\\ a_{1\ j}^{0\ i}=0 & \text{if } j \text{ is odd},\\ a_{1\ j}^{1\ i}=0 & \text{if } i \text{ or } j \text{ is even}\end{cases}\tag{2.5}$$

である。$q=m-1$ の場合または $m=4p$ かつ $q=2p\pm1$ の場合には $\sigma^2=1$ を満たしているから、(2.4)より

$$\begin{aligned}a_{0\ 2l-1}^{1\ 2k}&=(a_{1\ 2l-1}^{1\ 1})^k(a_{1\ \sigma(2l-1)}^{1\ 1})^k\zeta^{n(2l-1)(2k-1)k},\\ a_{1\ 2l}^{0\ 2k-1}&=(a_{1\ 1}^{1\ 2k-1})^l(a_{1\ 1}^{1\ \sigma(2k-1)})^l\zeta^{n(2k-1)(2l-1)l},\\ a_{1\ 2l-1}^{1\ 2k-1}&=(a_{1\ 2l-1}^{1\ 1})^k(a_{1\ \sigma(2l-1)}^{1\ 1})^{k-1}\zeta^{n(2l-1)(2k-1)k}\\ &=(a_{1\ 1}^{1\ 2k-1})^l(a_{1\ 1}^{1\ \sigma(2k-1)})^{l-1}\zeta^{n(2k-1)(2l-1)l}\end{aligned}\tag{2.6}$$

が任意の $k,l=1,2,\cdots,[\frac{m}{2}]$ に対して成立する。実数 x に対して、$[x]$ は x を超えない最大の整数を表す。特に、

$$\begin{cases}a_{1\ 1}^{1\ 2k-1}= & (a_{1\ 1}^{1\ 1})^k(a_{1\ \sigma(1)}^{1\ 1})^{k-1}\zeta^{n(2k-1)k},\\ a_{1\ 2l-1}^{1\ 1}= & (a_{1\ 1}^{1\ 1})^l(a_{1\ 1}^{1\ \sigma(1)})^{l-1}\zeta^{n(2l-1)l}\end{cases}\tag{2.7}$$

となる。これより、$a := a_{11}^{11} = 0$ ならば、$(\alpha,\beta) \neq (0,0)$ なる任意の $\alpha,\beta = 0,1$ と任意の $i,j = 0,1,\cdots,m-1$ に対して $a_{\beta}^{\alpha}{}_{j}^{i} = 0$ となり、R は $< s >$ の普遍R行列となることがわかる。以下、証明の最後まで $a = a_{11}^{11} \neq 0$ と仮定する。

(❶)において $\alpha = \beta = 1, \alpha' = 0, i = 0, j = k = 1$ とすると

$$0 = a_0^1{}_1^1{}_{\sigma(1)} a_1^0{}_1^0 + a_1^1{}_1^1 a_0^0{}_1^0$$

となるが、(2.5)から $a_1^0{}_1^0 = 0$ であり、仮定から $a \neq 0$ なので、$a_0^0{}_1^0 = 0$ を得る。一方、$(\varepsilon \otimes id)(R) = 1$ を満たさなければならないので、

$$a_0^0{}_1^0 + a_0^1{}_1^0 = 1$$

を得る。また、(2.4)において $\beta = 0$, $i = m-1, j = 1$ にとることにより

$$a_0^1{}_1^0 = \delta_{0,m} (a_1^1{}_1^1)^{[\frac{m-1}{2}]+1} (a_1^1{}_1^{\sigma(1)})^{[\frac{m}{2}]} \zeta^{n\frac{m(m-1)}{2}}$$

を得る。まとめると

$$\delta_{0,m} (a_1^1{}_1^1)^{[\frac{m-1}{2}]+1} (a_1^1{}_1^{\sigma(1)})^{[\frac{m}{2}]} \zeta^{n\frac{m(m-1)}{2}} = 1 \tag{2.8}$$

が得られる。この等式から、$a_1^1{}_1^{\sigma(1)} \neq 0$ でなければならない。よって、任意の $k,l = 1,2,\cdots,[\dfrac{m}{2}]$ に対して、$a_1^1{}_1^{2k-1}$, $a_1^1{}_{2l-1}^1$ は 0 でないことがわかる。

(❶)において $\alpha = \beta = 1, \alpha' = 0, k = 1$ にとることにより、

$$0 = a_0^1{}_1^1{}_{\sigma^{-1}(j)} a_1^0{}_j^i + a_1^1{}_j^1 a_0^0{}_j^i$$

を得るが、j が奇数ならば、$a_1^0{}_j^i = 0$、$a_1^1{}_j^1 \neq 0$ なので $a_0^0{}_j^i = 0$ を得る。同様に(❶)′ から i が奇数ならば $a_0^0{}_j^i = 0$ を得る。結局、

$$a_0^0{}_j^i = 0 \quad \text{if } i \text{ or } j \text{ is odd} \tag{2.9}$$

が得られた。

I. $q = m-1$ の場合：m が奇数ならば、(2.8)式が成り立たないから、m は偶数でなければならない。$m \neq 4$ の場合は、(❶)により $a_1^1{}_1^1 = 0$ となるので、仮定に反する。

$m = 4$ の場合を考える。$i = 0,1,2,3$ に対して、

$$\sigma(i) \equiv -i \pmod 4$$

である。(2.8)から

$$a^2 (a_1^1{}_1^3)^2 \zeta^{2n} = 1 \cdots\cdots (❺)$$

である。一方、(2.6)の $a_1^1{}_{2l-1}^{2k-1}$ に関する等式において $k = 2, l = 1$ の場合を考えて、

$$a^2 = \zeta^n \qquad \cdots\cdots (❻)$$

を得る。同じく(2.6)から

$$a_1^{1\ 3}_{\ 3} = (a_1^{1\ 1}_{\ 3})^2 (a_1^{1\ 1}_{\ 1})^1 \zeta^{9n}$$

となるが、(❸)により $a_1^{1\ 3}_{\ 3} = a_1^{1\ 1}_{\ 1}$ なので、

$$(a_1^{1\ 1}_{\ 3})^2 = \zeta^{-n} \qquad \cdots\cdots(❼)$$

を得る。(❺)(❻)(❼)から $\zeta^{2n} = 1$ を得るので、n は偶数でなければならない。

以下、n は偶数とする。このとき、(❻)より $a^2 = (\pm 1)^{\frac{n}{2}}$ であり、(❼)より

$$a_1^{1\ 3}_{\ 1} = a\nu \quad (\text{但し、} \nu = \pm 1)$$

とおくことができる。以上の考察と(2.6)から

$$a_{1j}^{1i} = \begin{cases} a\nu & \text{if } (i,j) = (1,3),\ (3,1) \\ a & \text{if } (i,j) = (1,1),\ (3,3)\ , \\ 0 & \text{otherwise} \end{cases} \quad a_{0j}^{1i} = a_{1i}^{0j} = \begin{cases} 1 & \text{if } (i,j) = (0,1),\ (0,3) \\ \nu & \text{if } (i,j) = (2,1),\ (2,3) \\ 0 & \text{otherwise} \end{cases}$$

となることがわかる。(❹)より $k,l = 1,2$ に対して

$$a_0^{0\ 2k}_{\ 2l} = \sum_{\beta=0,1} a_\beta^{0\ 1}_{\ \sigma-\beta(2l)} a_\beta^{0\ 2k-1}_{\ 2l} = a_0^{0\ 1}_{\ 2l} a_0^{0\ 2k-1}_{\ 2l} + a_1^{0\ 1}_{\ 2l} a_1^{0\ 2k-1}_{\ 2l} = 1$$

となる。以上より、$q = m-1$ かつ $a = a_1^{1\ 1}_{\ 1} \neq 0$ の場合には n は偶数であり、

$$R = \sum_{\substack{\alpha,\beta=0,1 \\ k,l=1,2}} a^{\alpha\beta} \nu^{\beta l + \alpha k} t^\alpha E_{2k-\beta} \otimes t^\beta E_{2l-\alpha}$$

但し、$a^2 = (-1)^{\frac{n}{2}}$, $\nu = \pm 1$ と書けていることがわかった。逆に、この形の R は $\mathbf{C}[D_{m,n,m-1}]$ の普遍R行列になっていることが確かめられる。

Ⅱ. $m = n = 4p$ かつ $q = 2p \pm 1$ $(p \geq 3)$ の場合： $q = 2p-1$ の場合は $k = 1, \cdots, 2p$ に対して

$$\sigma(2k) = 4p - 2k,$$
$$\sigma(2k-1) \equiv 2p - 2k + 1 \pmod{m}$$

となる。$q = 2p+1$ の場合は $k = 1, \cdots, 2p$ に対して

$$\sigma(2k) = 2k,$$
$$\sigma(2k-1) \equiv 2p + 2k - 1 \pmod{m}$$

となる。いずれにしても $\sigma(\{1,3,\cdots,4p-1\}) = \{1,3,\cdots,4p-1\}$ が成り立っている。このことと(2.4)と(2.9)から $a_\beta^{\alpha\ i}_{\ j}$ $(\alpha,\beta = 0,1,\ i,j = 0,1,\cdots,m-1)$ のうち

$$a_0^{0\ 2k}_{\ 2l},\ a_0^{1\ 2k}_{\ 2l-1},\ a_1^{0\ 2k-1}_{\ 2l},\ a_1^{1\ 2k-1}_{\ 2l-1} \quad (k,l = 1,2,\cdots,2p)$$

以外はすべて 0 になることがわかる。

(2.8)より $(aa_1^{1\ 1}{}_{\sigma(1)})^{2p}=1$ であるから

$$aa_1^{1\ 1}{}_{\sigma(1)}=\omega \quad (\text{但し、}\omega\text{ は }1\text{ の }2p\text{ 乗根})$$

とおくことができる。よって、

$$a_1^{1\ \sigma(1)}{}_1=a_1^{1\ 1}{}_{\sigma(1)}=a^{-1}\omega \tag{2.10}$$

となる。(2.7)より任意の $k,l=1,2,\cdots,2p$ に対して

$$a_1^{1\ 2k-1}{}_1=a\omega^{k-1},\qquad a_1^{1\ 1}{}_{2l-1}=a\omega^{l-1} \tag{2.11}$$

となる。(2.10)と(2.11)から

$$a^2\omega^{\frac{q-3}{2}}=1$$

を得る。これを用いて、(2.6)より任意の $k,l=1,2,\cdots,2p$ に対して

$q=2p-1$ の場合	$q=2p+1$ の場合
$a_0^{1\ 2k}{}_{2l-1}=\omega^k$	$a_0^{1\ 2k}{}_{2l-1}=\omega^{2kl-k}$
$a_1^{0\ 2k-1}{}_{2l}=\omega^l$	$a_1^{0\ 2k-1}{}_{2l}=\omega^{2kl-l}$
$a_1^{1\ 2k-1}{}_{2l-1}=a\omega^{k+l-2}$	$a_1^{1\ 2k-1}{}_{2l-1}=a\omega^{2kl-k-l}$

となることがわかる。そして、(❹)より $k,l=1,2\cdots,2p$ に対して、

$$\begin{cases} q=2p-1\ \text{のとき} & a_0^{0\ 2k}{}_{2l}=\sum_{\beta=0,1}a_\beta^{0\ 1}{}_{\sigma^{-\beta}(2l)}a_\beta^{0\ 2k-1}{}_{2l}=1,\\ q=2p+1\text{のとき} & a_0^{0\ 2k}{}_{2l}=\sum_{\beta=0,1}a_\beta^{0\ 1}{}_{\sigma^{-\beta}(2l)}a_\beta^{0\ 2k-1}{}_{2l}=\omega^{2kl}\end{cases}$$

となる。結局、$m=n=4p$ かつ $q=2p-1$ かつ $a=a_1^{1\ 1}\neq 0$ の場合には

$$R=\sum_{\substack{\alpha,\beta=0,1\\ k,l=1,2,\cdots,2p}} a^{\alpha\beta}\omega^{\alpha k+\beta l-2\alpha\beta}t^\alpha E_{2k-\beta}\otimes t^\beta E_{2l-\alpha},$$

$m=n=4p$ かつ $q=2p-1$ かつ $a=a_1^{1\ 1}\neq 0$ の場合には

$$R=\sum_{\substack{\alpha,\beta=0,1\\ k,l=1,2,\cdots,2p}} a^{\alpha\beta}\omega^{2kl-\beta l-\alpha k}t^\alpha E_{2k-\beta}\otimes t^\beta E_{2l-\alpha}$$

と書けていることがわかった。ここで、$a^2=\omega^{-\frac{q-3}{2}}$, ω は 1 の $2p$ 乗根である。逆に、この形の R は $\mathbf{C}[D_{m,n,q}]$ の普遍R行列になっていることが確かめられる。$\omega=\zeta^{2c}$ $(c=0,1,\cdots,2p-1)$ とおいて、(2.1) を使って、上式の右辺を s と t で書き直せば、定理2の(ii)(iii)の式になる。□

§.3 包括的注意

定理2の新しい普遍R行列を使って、意味のある絡み目の不変量を導くことはできなかったが、これらの普遍R行列に関して少しだけ興味深いことがある。それは、普遍R行列(の族)が位数8の二面体群 D_8 と四元数群 Q_8 を区別する情報を持っているということである。

D_8 と Q_8 は、群としては同型でないが、それらの表現環は同型であることでよく知られている。群として同型でないことは、D_8 には位数2の元が5個あるが、Q_8 には1個しかないことからすぐにわかる。D_8 と Q_8 の表現環が同型であることは、それらの指標表が一致することからすぐにわかる。

さて、(A,R) を準三角ホップ代数とし、その普遍R行列 R を $R=\sum_i \alpha_i \otimes \beta_i$ と書く。このとき、

$$u := \sum_i S(\beta_i)\alpha_i$$

という A の元を考える。ここで、S はホップ代数 A の対合である。u の A への左作用から定まる線形変換のトレースは Majid[6]によって準三角ホップ代数 (A,R) の階数と呼ばれ、よく研究されている。階数は準三角ホップ代数の不変量である。実は、この階数を $\mathbf{C}[D_8]$ と $\mathbf{C}[Q_8]$ のすべての普遍R行列について計算することにより、D_8 と Q_8 が同型な群でないことが再証明される[14]。

まだ、あまり詳しく調べていないが、普遍R行列(の族)を使って、有限群やホップ代数の分類に役立てることができる可能性がある。このあたりをはっきりさせることは、将来の課題の1つである。

参考文献

[1] E. Abe "Hopf algebras", Cambridge University Press, Cambridge, 1980 (original Japanese version published by Iwanami Shoten, Tokyo, 1977)

[2] C. W. Curtis and I. Reiner "Methods of representation theory volume 1", John Wiley & Sons, 1981

[3] V. G. Drinfel'd "Quantum groups", in "Proceedings of the International Congress of Mathematics, Berkeley, CA., 1987" p.798—820

[4] V. G. Drinfel'd "On almost cocommutative Hopf algebras" Leningrad Math. J. 1 (1990) p.321—342

[5] M. Jimbo "A q-difference analogue of $U_q(g)$ and the Yang-Baxter equation" Lett. Math. Phys. **10** (1985) p.63—69

[6] S. Majid "Representation-theoretic rank and double Hopf algebras" Comm. Alg. **18** (1990) p.3705—3712

[7] H. Murakami, T. Ohtsuki and M. Okada "Invariants of three manifolds derived from linking matrices of framed links" Osaka J. Math. **29** (1992) p.545—572

[8] D. E. Radford "On the antipode of a quasitriangular Hopf algebra" J. of Alg. **151** (1992) p.1—11

[9] D. E. Radford "On Kauffman's knot invariants arising from finite-dimensional Hopf algebras" in "Advances in Hopf algebras" (Lecture Notes in Pure and

Applied Mathematics 158), edited by J. Bergen and S. Montgomery, Marcel Dekker, 1994, p.205—266
[10] N. Yu. Reshetikhin and V. G. Turaev "Ribbon graphs and their invariants derived from quantum groups" Comm. Math. Phys. **127** (1990) p.1—26
[11] N. Yu. Reshetikhin and V. G. Turaev "Invariants of 3-manifolds via link polynomials and quantum groups" Invent. Math. **103** (1991) p.547—597
[12] M. -C. Shum "Tortile tensor category" J. Pure and Appl. Math. **93** (1994) p.57—110
[13] M. Suzuki "Group theory I, II" , Springer-Verlag, 1982, 1986(original Japanese version published by Iwanami Shoten, Tokyo, 1977, 1978)
[14] M. Wakui "二面体群の普遍R行列について" to appear in 数理解析研究所講究録

†：彼らは、タングルダイアグラム(＝絡み目のダイアグラムを高さ関数によって輪切りにしたときに得られる各ピース)を射とする圏 OTD が「豊かな構造」を持つことに注目した。そして、圏 OTD からホップ代数の表現のなす圏への「豊かな構造」を保つ関手が構成されるためのホップ代数に対する十分条件として、リボンホップ代数という概念を導いた。現在では、圏 OTD の持つ「豊かな構造」は完全に解析され、そのような構造を持つ圏は tortile 圏と呼ばれている。OTD は1つの対象で生成される tortile 圏の中で最も普遍的な圏として特徴づけられる[12]。

††：ζ を 1 の原始 m 乗根、$\epsilon = 1, 2$ として $E_k^{(\epsilon)} := \dfrac{1}{m} \sum_{i=0}^{m-1} \zeta^{-ik} s_\epsilon^i$ とおき、基底として

$$\{t^\alpha E_i^{(1)} E_j^{(2)} \mid \alpha = 0, 1,\ i, j = 0, 1, \cdots, m-1\}$$

を選んで計算する。

The number of p-th roots of unity in a symmetric group

Yugen Takegahara (竹ヶ原　裕元)
Muroran Institute of Technology (室蘭工業大学)

For a prime p, define positive integers $a(n)$ $(n = 0, 1, 2, \ldots)$ by

$$\sum_{n=0}^{\infty} \frac{a(n)}{n!} x^n = \exp\left(x + \frac{x^p}{p}\right).$$

Then

$$a(n) = \sum_{k=0}^{[n/p]} \frac{n!}{(n-kp)!k!p^k} = \begin{cases} \sharp\{x \in S_n | x^p = 1\} & n \geq 1, \\ 1 & n = 0, \end{cases}$$

where S_n is the symmetric group on n letters. It follows from [3] that

$$(*) \qquad a(n) = a(n-1) + \frac{(n-1)!}{(n-p)!} a(n-p).$$

If $p = 2$ and if $n \geq 4s - 2$, then 2^s divides $a(n)$ by this formula ([2]). The following results are well known.

Wilson's Theorem

$$a(p) = 1 + (p-1)! \equiv 0 \bmod p$$

Frobenius Theorem

$$a(n) \equiv 0 \bmod p, \qquad n \geq p$$

The p-adic power series

$$E_p(x) = \exp\left(\sum_{i=0}^{\infty} \frac{x^{p^i}}{p^i}\right) \in \mathbb{Z}_p[[x]]$$

is called Artin-Hasse exponential. One of the important property is that $E_p(x) \in \mathbb{Z}_p[[x]]$. It follows that

$$\sum_{n=0}^{\infty} \frac{a(n)}{n!} x^n = \exp\left(x + \frac{x^p}{p}\right) = E_p(x) \prod_{i=2}^{\infty} \exp\left(-\frac{x^{p^i}}{p^i}\right).$$

Using this fact, we have that

$$\mathrm{ord}_p\left(\frac{a(n)}{n!}\right) \geq -\frac{n}{p^2}\left(2 + \frac{1}{p-1}\right)$$

([7]), or equivalently,

$$\mathrm{ord}_p(a(n)) \geq \sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right] - \frac{n}{p^2}\left(2 + \frac{1}{p-1}\right).$$

Our purpose is to determine $\mathrm{ord}_p(a(n))$, which is the exponent of p in the decomposition of $a(n)$ into prime factors.

Definition 1

$$\gamma(n) = \left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right]$$

By the preceding result, if $p = 2$, $\mathrm{ord}_2(a(n)) \geq \gamma(n)$. Moreover, the formula $(*)$ implies the following.

Theorem 1 ([4]) *For each n, let $y_n = [n/p^2]$.*

(1) $\mathrm{ord}_p(a(n)) \geq \gamma(n)$

(2) $\dfrac{a(n)}{p^{\gamma(n)}} \equiv (-1)^{y_n} \dfrac{a(r)}{p^{\gamma(r)}} \bmod p, \quad r = n - p^2 y_n$

(3) $\mathrm{ord}_p(a(kp^2)) = \gamma(kp^2) = k(p-1)$

For a prime p and for a positive integer l, define positive integers $a(n,l)$ $(n = 0, 1, 2, \ldots)$ by

$$\sum_{n=0}^{\infty} \frac{a(n,l)}{n!} x^n = \exp\left(\sum_{i=0}^{l} \frac{x^{p^i}}{p^i}\right).$$

Then

$$a(n,l) = \sharp\{x \in S_n | x^{p^l} = 1\} \quad (n \geq 1), \quad a(0,l) = 1.$$

As a generalization of Theorem 1, we get the following.

Theorem 2 ([6]) *For each n, let $y_n = [n/p^{l+1}]$, and let $f_p^l(n) = \sum_{j=1}^{l} [n/p^j]$.*

(1) $\mathrm{ord}_p(a(n,l)) \geq f_p^l(n) - l y_n$,

(2) $a(n,l) \equiv \dfrac{(-1)^{y_n} n!}{p^{(l+1)y_n} y_n! (n - p^{l+1} y_n)!} a(n - p^{l+1} y_n, l) \bmod p^{f_p^l(n) - l y_n + l + 1}$,

(3) $\mathrm{ord}_p(a(kp^{l+1}, l)) = k(p^l + p^{l-1} + \cdots + p - l)$

In particular,

$$a(n) \equiv \frac{(-1)^{y_n} n!}{p^{2y_n} y_n! (n - p^2 y_n)!} a(n - p^2 y_n) \bmod p^{\gamma(n)+2}, \quad y_n = \left[\frac{n}{p^2}\right].$$

To prove Theorem 2, we use the property of Artin-Hasse exponential: $E_p(x) \in \mathbb{Z}_p[[x]]$([6]).

Corollary 1 *The p-adic exponential function*

$$\exp\left(\sum_{i=0}^{l} \frac{x^{p^i}}{p^i}\right)$$

converges only in the open disc of radius

$$p^{-\frac{p+l(p-1)}{p^{l+1}(p-1)}}.$$

Corollary 2 *For a nonnegative integer r less than p^2,*

$$\begin{aligned} &\mathrm{ord}_p(a(kp^2+r)) = \gamma(kp^2) + \mathrm{ord}_p(a(r)) && \text{if } \mathrm{ord}_p(a(r)) \le \gamma(r)+1, \\ &\mathrm{ord}_p(a(kp^2+r)) \ge \gamma(kp^2+r) + 2 && \text{otherwise.} \end{aligned}$$

When $p < 300$,

$$\mathrm{ord}_p(a(r)) \le \gamma(r) + 2$$

for any nonnegative integer r less than p^2.

Example([4, 6, 8]) Let $p = 2$. Then

$$a(0) = 1, \quad a(1) = 1, \quad a(2) = 2, \quad a(3) = 4,$$

$$\mathrm{ord}_2(a(n)) = \begin{cases} \gamma(n)+1 & \text{if } n \equiv 3 \bmod 4, \\ \gamma(n) & \text{otherwise.} \end{cases}$$

If $\mathrm{ord}_p(a(n)) = \gamma(n) + m$, m is called the *type* of n for p. If $\mathrm{ord}_p(a(n)) \ge \gamma(n) + 2$, n is called *exceptional* integer for p.

Example([4, 8]) Let $p = 3$. Then

$$\begin{aligned} &a(3) = 3, && a(4) = 9, && a(5) = 21, \\ &a(6) = 81, && a(7) = 351, && a(8) = 1233. \end{aligned}$$

Hence, 6 is a unique exceptional integer less than 9.

$$\mathrm{ord}_3(a(n)) \ge \gamma(n)+3 \quad \text{if } n \equiv 24 \bmod 27,$$

$$\mathrm{ord}_3(a(n)) = \begin{cases} \gamma(n)+2 & \text{if } n \equiv 6 \bmod 27 \text{ or if } n \equiv 15 \bmod 27, \\ \gamma(n)+1 & \text{if } n \equiv 4 \bmod 9 \text{ or if } n \equiv 7 \bmod 9, \\ \gamma(n) & \text{otherwise.} \end{cases}$$

Especially,

$$\begin{aligned} &a(15) = 168369111, && a(24) = 13428028220072049, \\ &\mathrm{ord}_3(a(15)) = 6 = \gamma(15)+2, && \mathrm{ord}_3(a(24)) = 10 = \gamma(24)+4. \end{aligned}$$

A *transfer matrix* $T(x) = (t_{ij}(x))_{1 \le i,j \le p}$ is a $p \times p$ matrix uniquely determined by the formula $(*)$ such that

$$\begin{pmatrix} a((k+1)p^2) \\ a((k+1)p^2+1) \\ \vdots \\ a((k+1)p^2+p-1)) \end{pmatrix} = p^{p-1} T(k) \begin{pmatrix} a(kp^2) \\ a(kp^2+1) \\ \vdots \\ a(kp^2+p-1) \end{pmatrix}$$

for any nonnegative integer k. In [8], Ochiai considered the following condition.

Condition A :

(1) $t_{ij}(x) \in \mathbb{Z}[x]$

(2) $t_{ij}(x) \equiv t_{1j}(x) \bmod p$ for any i and j

(3) $t_{11}(x) + t_{22}(x) + \cdots + t_{pp}(x) \not\equiv 0 \bmod p$

Theorem 3 ([8]) *Suppose p be a prime satisfying Condition A. Then there exist p-adic analytic functions*

$$\lambda(x) \in \mathbb{Z}_p[[x]] \text{ and } f_r(x) \in \mathbb{Z}_p[[x]]$$

for $r = 0, 1, \ldots, p^2 - 1$ convergent on $\{x | \mathrm{ord}_p(x) \geq 0\}$ such that

$$a(kp^2 + r) = p^{k(p-1)} f_r(k) \prod_{j=1}^{k} \lambda(j)$$

for any nonnegative integer k. In particular,

$$\mathrm{ord}_p(a_p(kp^2 + r)) = k(p-1) + \mathrm{ord}_p(f_r(k)).$$

Proposition 1 ([5]) *Any prime p satisfies Condition (A); moreover,*

$$(1)' \quad t_{ij}(x) \in \mathbb{Z} + p\mathbb{Z}[x]$$
$$(3)' \quad t_{11}(x) + t_{22}(x) + \cdots + t_{pp}(x) \equiv -1 \bmod p$$

Moreover, we have the following.

Theorem 4 *Let r be a positive integer less than p^2. If $r \geq p$, then there exist integers c and d that are divisible by $p^{\gamma(r)+2}$ such that*

$$a(kp^2 + r) \equiv \left(1 - p! \sum_{1 \leq w \leq \gamma(r)} w^{-1} k\right) a(r) a(kp^2) + (-1)^k p^{k(p-1)}(ck + dk^2) \bmod p^{\gamma(kp^2+r)+3}.$$

for any nonnegative integer k.

Using these results and Hensel's lemma, we get the following.

Theorem 5 *Assume that $\mathrm{ord}_p(a(r)) = \gamma(r) + 2$ for a positive integer r less than p^2. Then there exist p-adic integers s and t such that*

$$\mathrm{ord}_p(a(kp^2 + r)) = \gamma(kp^2 + r) + 2 + \mathrm{ord}_p(1 + sk + tk^2)$$

for any positive integer k.

When $p < 300$, the type of each exceptional integer less than p^2 is 2, and there is no exceptional integer in each of the cases where

$$\begin{aligned} p = \; & 2, 5, 13, 17, 31, 43, 67, 73, 79, 83, \\ & 101, 113, 137, 149, 173, 179, 193, 197, 199, \\ & 233, 241, 251, 257, 271, 281. \end{aligned}$$

Let r be a positive integer of type 2 less than p^2. Put $\bar{b} = p^{-\gamma(r)-2} a(r)$. By Theorem 4, there exist nonnegative integers $\bar{c}$ and $\bar{d}$

$$a(kp^2 + r) \equiv (-1)^k p^{\gamma(kp^2+r)+2}(\bar{b} + \bar{c}k + \bar{d}k^2) \bmod p^{\gamma(kp^2+r)+3}.$$

Example([8]) Let $p = 3$. Then

$$a(9k+6) \equiv (-1)^k 3^{\gamma(9k+6)+2}(1+k) \bmod p^{\gamma(9k+6)+3},$$
$$\mathrm{ord}_3(a(9k+6)) = 2k+4+\mathrm{ord}_3(u+k),$$

where

$$u \equiv 1+2\cdot 3+3^2+2\cdot 3^3+2\cdot 3^4+2\cdot 3^5+2\cdot 3^6+3^8+2\cdot 3^9 \bmod 3^{14}.$$

Especially,

$$\mathrm{ord}_3(a(105)) = 26+7 = 33 = \gamma(105)+9.$$

Example([5]) Let $p = 23$. Then 127 is a unique exceptional integer less than 529, the type of which is 2. We have that

$$a(529k+127) \equiv (-1)^k 23^{\gamma(529k+127)+2}\cdot 6$$

and that

$$\mathrm{ord}_p(a(n)) = \begin{cases} \gamma(n)+2 & \text{if } n \equiv 127 \bmod 529, \\ \gamma(n)+1 & \text{if } n \equiv 92, 114, 217, 233, 243, 286, 381, 402, \\ & \qquad 420, 484, 494, 511, 514 \bmod 529, \\ \gamma(n) & \text{otherwise.} \end{cases}$$

Ishihara decides all exceptional integers for $p < 300$.

Exceptional integers r less than p^2 for $p < 100$

p	r	$\gamma(r)$	type	$\bar{b}+\bar{c}k+dk^2$
3	6	2	2	$1+k$
7	28	4	2	$6+6k$
	48	6	2	1
11	49	4	2	$3+3k$
	58	5	2	$10+9k$
19	55	2	2	$15+13k$
	249	13	2	$15+16k$
23	127	5	2	6
29	259	8	2	$9+k$
37	1348	36	2	$10+22k$
41	1264	30	2	$30+33k$
47	2099	44	2	$26+32k$
53	2075	39	2	$1+46k$
59	714	12	2	$42+47k$
	2885	48	2	$27+26k$
61	690	11	2	$6+25k$
71	2859	40	2	$16+70k$
89	3544	39	2	$14+66k$
97	3894	40	2	$22+45k$

When $p < 300$, the answers of the following questions are '*yes*'.

Question 1 For any exceptional integer r of type 2 such that $p \leq r < p^2$, does there exist an integer $b(r)$ such that $b(r) \equiv 0 \bmod p^{\gamma(r)+2}$ and that

$$a(kp^2 + r) \equiv (-1)^k p^{k(p-1)}(a(r) + b(r)k) \bmod p^{\gamma(kp^2+r)+3}$$

for each nonnegative integer k?

Question 2 Is the type of any exceptional integer less than p^2 necessarily 2 for all primes?

Question 3 Does there necessarily exist any integer of type 1 for all primes p?

If Wilson quotient $w_p = \dfrac{1 + (p-1)!}{p}$ is divisible by p, i.e., $\mathrm{ord}_p(a(p)) \geq 2$, then p is called *Wilson prime*. It follows from [1] that all of Wilson prime less than 5×10^8 are

$$5, 13, \text{ and } 563.$$

Therefore, $a(p) \leq 2$ for $p < 5 \times 10^8$. Finally, we present the following conjecture.

Conjecture For any n such that $n \geq p^2$, $\mathrm{ord}_p(a(n)) < \mathrm{ord}_p(n!)$.

References

[1] R. Crandall, K. Dilcher and C. Pomerance, A search for Wieferich and Wilson primes, *Mathematics of Computation* 66 (1997), 433-449.

[2] S. Chowla, I. N. Herstein and W. K. Moore, On recursions connected with symmetric groups 1, *Canadian Journal of Mathematics* 3 (1951), 328-344.

[3] S. Chowla, I. N. Herstein and W.R.Scott, The solutions of $x^d = 1$ in symmetric groups, *Norske Vid. Selsk. Forh. (Trondheim)*, 25 (1952), 29–31.

[4] A. W. M. Dress and T. Yoshida, On p-divisibility of the Frobenius numbers of symmetric groups, preprint.

[5] H. Ishihara, H. Ochiai, Y. Takegahara and T. Yoshida, On the power of a prime p dividing the number of solutions of $x^p = 1$ in a symmetric group, preprint.

[6] H. Katsurada, Y. Takegahara and T. Yoshida, The number of homomorphisms from a finite abelian group to a symmetric group, submitted to Comm. Algebra.

[7] S. Lang, Cyclotomic Fields I and II, Springer–Verlag, New York, 1990.

[8] H. Ochiai, A p-adic property of Taylor series of $\exp(x + x^p/p)$, Hokkaido math. J., accepted.

On Sylow Subgroups of an Abelian Group Containing an Affine Difference Set

Agnes v. Dizon-Garciano
Mathematics Department, Ateneo de Manila University, Loyola Heights, Quezon City, the Philippines

Yutaka Hiramine
Department of Mathematics, Faculty of Education, Kumamoto University, Kurokami, Kumamoto, Japan

1. Introduction

Affine difference sets are a special class of general relative difference sets introduced in Elliot and Butson [4]. Its parameters are of the form $(n+1, n-1, n, 1)$ where $n(>1)$ is a positive integer. In Dembowski and Piper [3], a classification of finite projective planes admitting quasiregular collineation groups is given. In the case that the plane admits a group G of type (d) in this classification, the incidence structure π consisting of the points and lines in the maximal orbit forms an $(n+1, n-1, n, 1)$ divisible design with a Singer group G, and hence can be described by some affine difference set.

The aim of this paper is to present some information on the structure of abelian groups containing affine difference sets. It is a well-known conjecture that if D is an affine difference set in an abelian group G, then for every prime p, the Sylow p-subgroup of G is cyclic. In Arasu and Pott [1], it was shown that the above conjecture is true when $p = 2$.

Theorem 1. (Arasu and Pott [1]) *Let D be an abelian affine difference set in G. Then the Sylow 2-subgroup of G is cyclic.*

We denote by $\pi(m)$ the set of primes dividing an integer m. For a set of primes π_0 and a positive integer m, we denote by m_{π_0} the π_0-part of m. If $\pi_0 = \phi$, then we set $m_{\pi_0} = 1$. For a positive integer s, we set $G_s = \{x \in G \mid x^s = 1\}$. If G is an abelian, then G_s is a subgroup of G.

In section 3, we present the following theorem concerning the Sylow p-subgroup of G for a prime p such that $p|n+1$.

Theorem 4. *Let D be an abelian affine difference set of order n in a group G. Let p be a prime divisor of $n+1$ and let r be the p-rank of G. Assume that p divides $w+1$ for some $w>1$ such that $\pi(w) \subseteq \pi(n)$. Set $s=(w-1)_{\pi_0}$, where $\pi_0=\pi((w-1,n^2-1))$. Then,*

$$r \leq \log_p(|G_s|+2).$$

As a corollary, we have :

Corollary 1. *Let D be an abelian affine difference set of order n in a group G. Let p be a prime divisor of $n+1$ and let r be the p-rank of G. Assume that p divides $w+1$ for some integer $w>1$ such that $\pi(w) \subseteq \pi(n)$. Set $\pi_0=\pi((w-1,n^2-1))$. If the Hall π_0-subgroup of G is cyclic, then $r \leq \log_p((w-1)_{\pi_0}+2)$.*

Corollary 1, together with Theorem 1, gives the following.

Corollary 2. *Let D be an abelian affine difference set of order n in a group G and let p be a prime dividing $n+1$.*

(i) *Let w be a prime divisor of n. Suppose there exists a positive integer ℓ such that $p|w^\ell+1$ and $\pi(w^\ell-1,n^2-1)=\{2\}$. If $p^2>(w^\ell-1)_2+1$, then the Sylow p-subgroup of G is cyclic.*

(ii) *Suppose $2|n$ and $p|2^\ell+1$ for a positive integer ℓ. If $(2^\ell-1,n^2-1)=1$, then the Sylow p-subgroup of G is cyclic. In particular, if $3|n+1$, then the Sylow 3-subgroup of G is cyclic.*

When n is a power of an odd prime, we have :

Corollary 3. *Let D be an abelian affine difference set of order n in a group G. Let $n=w^e$ where w is an odd prime and e is a positive integer. If $3|n+1$, then the 3-rank of G is at most $\log_3(|G_{w-1}|+2)$.*

Throughout the article all sets and groups are assumed to be finite. Notations and teminology are standard and taken from [8].

2. Preliminaries

Let G be a finite group of order n^2-1 and let N be a normal subgroup of G of order $n-1$. Suppose D is an n-subset of G with the property that the list of differences $d_1d_2^{-1}(d_1,d_2 \in D, d_1 \neq d_2)$ contains each element of $G-N$ exactly once and no element of $N-\{1\}$. Then D is called an *affine difference set* of *order* n in G relative to N. An affine difference set D is said to be *abelian* or *cyclic* if the group G has the respective property.

Given a prime power q, (cyclic) affine difference sets of order q have been constructed (see Bose [2]). Basically, we consider the finite field $GF(q^2)$. The set $D=\{x \in GF(q^2) \mid \mathrm{trace}_{GF(q)}(x)=1\}$ is an affine difference set in the cyclic group $GF(q^2)^*$ under multiplication. These correspond to Desarguesian planes. Some non-abelian examples are given by Ganley and Spence [5] which also correspond to Desarguesian planes. In the abelian case, the only known examples are the cyclic ones given above, and these are of prime power order. Hoffman [6] conjectured that affine difference sets of other orders do not exist.

Let D be an affine difference set in a group G. Then the set $Dg=\{dg \mid d \in D\}$ is called a *translate* of D for each $g \in G$. A (numerical) *multiplier* of an abelian difference set D is an integer t relatively prime to n^2-1 satisfying $D^{(t)}=Dg$ for some $g \in G$. Here $D^{(t)}:=\{d^t|d \in D\}$. We shall use the following result which is essentially contained in [4].

Theorem 2.([4]) *Let D be an abelian affine difference set of order n in a group G. Let t be a positive integer such that $\pi(t) \subseteq \pi(n)$. Then t is a multiplier of D.*

Lemma 3. *Let B be a subset of an abelian group G such that $(|B|,|G|)=1$. Then there exists a translate C of B satisfying the following:*

If $C^{(t)}=Cu$ for some integer t and some $u \in G$, then $u=1$.

Proof. Let Γ be the set of translates of B and f a mapping from Γ into G defined by $f(Bx)=\prod_{z \in Bx} z$. We note that $f(Bx)=ax^k$, where $a=\prod_{z \in B} z$ and $k=|B|$. Assume $f(Bx)=f(By)$. Then $ax^k=ay^k$ and hence $(xy^{-1})^k=1$. By assumption, $(k,|G|)=1$. Therefore $xy^{-1}=1$ and so $x=y$. It follows that f is bijective as $|\Gamma|=|G|$. Thus there exists a unique translate of B, say C, satisfying $f(C)=1$.

Assume $C^{(t)} = Cu$ for some integer t and some $u \in G$. Then $f(Cu) = f(C)^t$. Since $f(Cu) = f(C)u^k$ and $f(C) = 1$, we have $u^k = 1$. As $(k, |G|) = 1$, $u = 1$. Thus the lemma holds.

If D is an abelian affine difference set of order n in G, then clearly Dg is again an affine difference set of G for each $g \in G$. As an application of Theorem 2 and Lemma 3, by exchanging D with a suitable translate, we can choose D such that

$(*)$ $\quad \pi(t) \subseteq \pi(n) \Longrightarrow D^{(t)} = D$

We now recall some facts about abelian groups. Let G be an abelian group and let p be a prime dividing $|G|$. We know that the set of p-elements forms the unique Sylow p-subgroup P of G. Furthermore, any abelian p-group (such as P) is the direct product of cyclic groups. Let $P = H_1 \times \cdots \times H_r$ where $H_i = \langle x_i \rangle, x_i \in P$. The integer r and the orders $|H_i|$ are uniquely determined (up to ordering). The integer r is called the *p-rank* of G. Clearly, an abelian p-group is cyclic if and only if its p-rank is 1.

3. The Structure of the Sylow p-subgroup of G

For the rest of this article, we assume that G is an abelian group of order $n^2 - 1$ and that D is an affine difference set of order n in G relative to a subgroup N of order $n - 1$.

In this section, we present the following theorem concerning the Sylow p-subgroup of G for a prime p such that $p|n + 1$.

Theorem 4. *Let D be an abelian affine difference set of order n in a group G. Let p be a prime divisor of $n+1$ and let r be the p-rank of G. Assume that p divides $w + 1$ for some $w > 1$ such that $\pi(w) \subseteq \pi(n)$. Set $s = (w - 1)_{\pi_0}$, where $\pi_0 = \pi((w - 1, n^2 - 1))$. Then,*

$$r \leq \log_p(|G_s| + 2).$$

Proof. By Theorem 2 and $(*)$ in section 2, we can choose D so that $D^{(w)} = D$. By Theorem 1, we may assume that $p > 2$.

Let $\Omega := \{x \in G | x^p = 1, x \neq 1\}$. Since $p|n+1$ and $|N| = n-1$, then for every element $x \in \Omega$, we have $x \notin N$. As D is an affine difference set in G, there exists a unique pair of elements $d_1, d_2 \in D$ such that $x = d_1 d_2^{-1}$. Now $x \in \Omega$ implies $x^p = 1$. From this, $x = x^{-w}$ as $p|w+1$. Thus, $d_1 d_2^{-1} = d_2^w (d_1^w)^{-1}$. Note that d_1^w and d_2^w are both in D because $D^{(w)} = D$. By definition of affine difference sets, we have either $d_1 = d_2$ or $d_1 = d_2^w$ and $d_2 = d_1^w$. But clearly, $d_1 \neq d_2$ as $x \neq 1$. Hence $d_1 = d_2^w$ and $d_2 = d_1^w$ hold. This gives us $x = d_2^{w-1}$. Thus, every element of Ω may be expressed as d^{w-1} for some $d \in D$. If $x = c^{w-1} = d^{w-1}$ for some $c \in D$, then $c^w c^{-1} = d^w d^{-1}$ and $c, d, c^w, d^w \in D$. Hence $c = d$. Thus d is uniquly determined by x.

Clearly $G_p = \Omega \cup \{1\}$, a maximal elementary abelian p-subgroup of G. Choose distinct elements $a, b \in \Omega$ and set

$$\Gamma = \{(u, v) \mid (a, b) \neq (u, v) \in \Omega \times \Omega, \quad uv^{-1} = ab^{-1}\}.$$

Since $(ab^{-1}, 1), (a, b), (1, ba^{-1}) \notin \Gamma$, we have $|\Gamma| = p^r - 3$.

Let $(u, v) \in \Gamma$ and set $t = w - 1$. By what we have proved above, there exist elements d_1, d_2, d_3, d_4 such that

$$a = d_1^t, \ b = d_2^t, \ u = d_3^t, \ v = d_4^t.$$

Set $z = (d_1 d_2^{-1})^{-1}(d_3 d_4^{-1})$. As $uv^{-1} = ab^{-1}$, we have $z^t = 1$. Set $t = ss'$, where $\pi(s) = \pi_0$ and $\pi(s') \cap \pi_0 = \phi$. Since the order of z is a divisor of $|G| = n^2 - 1$ and $(s', n^2 - 1) = 1$, it follows that $z^s = 1$. Thus $z \in G_s$ and so $d_3 d_4^{-1} \in G_s d_1 d_2^{-1}$. From this we have $|\Gamma| \leq |G_s d_1 d_2^{-1} - \{d_1 d_2^{-1}\}| = |G_s| - 1$. Hence $p^r - 3 \leq |G_s| - 1$ and so $p^r \leq |G_s| + 2$. Thus the theorem holds.

Let X be a group and Y a subgroup of X. Set $\pi_1 = \pi(|Y|)$. Y is called a *Hall π_1-subgroup* of X if $(|Y|, [X : Y]) = 1$. We note that the trivial group $\{1\}$ is a Hall ϕ-subgroup of X.

Corollary 1. *Let D be an abelian affine difference set of order n in a group G. Let p be a prime divisor of $n+1$ and let r be the p-rank of G. Assume that p divides $w+1$ for some $w > 1$ such that $\pi(w) \subseteq \pi(n)$. Set $\pi_0 = \pi((w-1, n^2-1))$. If the Hall π_0-subgroup of G is cyclic, then $r \leq \log_p((w-1)_{\pi_0} + 2)$.*

Proof. Set $s = (w-1)_{\pi_0}$ and let H be the Hall π_0-subgroup of G. By assumption, H is cyclic and therefore $|G_s| \leq s$. Applying Theorem 4, $r \leq \log_p(|G_s| + 2) \leq \log_p(s+2) = \log_p((w-1)_{\pi_0} + 2)$. Thus the corollary holds.

By Corollary 1, we have

Corollary 2. *Let D be an abelian affine difference set of order n in a group G and let p be a prime dividing $n+1$.*

(i) *Let w be a prime divisor of n. Suppose there exists a positive integer ℓ such that $p|w^\ell+1$ and $\pi(w^\ell-1, n^2-1)=\{2\}$. If $p^2>(w^\ell-1)_2+2$, then the Sylow p-subgroup of G is cyclic.*

(ii) *Suppose $2|n$ and $p|2^\ell+1$ for a positive integer ℓ. If $(2^\ell-1, n^2-1)=1$, then the Sylow p-subgroup of G is cyclic. In particular, if $3|n+1$, then the Sylow 3-subgroup of G is cyclic.*

Proof. (i) follows immediately from Corollary 1. Under the condition of (ii) assume $(2^\ell-1, n^2-1)=1$. Then, by Corollary 1, the p-rank of G is at most $\log_p(1+2)\leq 1$. On the other hand, if $3|n+1$, then the 3-rank of G is at most $\log_3(1+2)=1$ since $3|2+1$. Thus (ii) holds.

Example 1. (i) Let $n=3^{4e+2}$ and D an abelian affine difference set of order n in a group G of order n^2-1. Then, since $5|3^2+1$, $5|n+1$ and $\pi((3^2-1, n^2-1))=\{2\}$ and since the Sylow 2-subgroup of G is cyclic by Theorem 1, Corllary 1 says that the 5-rank of G is at most $\log_5(8+2)<2$. Thus the Sylow 5-subgroup of G is cyclic. Note that if $5^b \mid 2e+1$ then $5^{b+1} \mid |G|$ (cf. Theorem 6.3 of [7]).

(ii) Let $n=5^{2e+1}$ and D an abelian affine difference set of order n in a group G of order n^2-1. Then, since $3|5+1$, $3|n+1$ and $\pi((5-1, n^2-1))=\{2\}$ and since the Sylow 2-subgroup of G is cyclic by Theorem 1, Corllary 1 says that the 3-rank of G is at most $\log_3(4+2)<2$. Thus the Sylow 3-subgroup of G is cyclic of order at least 3^{b+1}, where $3^b|2e+1$ (cf. Theorem 6.3 of [7]).

(iii) Let p and q be primes such that $q=2p+1\equiv 2 (\mathrm{mod}\ 3)$ and let $n=p^aq^b$, where $a+b\equiv 1(\mathrm{mod}\ 2)$. Then $3|n+1$ and $3|q+1$. Since $(q-1, n^2-1)=(2p, p^{2a}q^{2b}-1)=2$, the 3-rank of G is at most $\log_3(2+2)<2$ by Corollary 1. Thus Sylow 3-subgroup of G is cyclic. Note that $3^2 \mid |G|$ when $a\equiv 3 (\mathrm{mod}\ 6)$ and $b\equiv 0 (\mathrm{mod}\ 6)$.

Example 2. Let $n=10646(=2\cdot 5323)$. Then $n+1=3^2\cdot 7\cdot 13^2$ and $|G|=3^2\cdot 5\cdot 7\cdot 13^2\cdot 2129$. As $2|n$ and $3|2+1$, the Sylow 3-subgroup of G is cyclic by Corollary 2 (ii). Since $13 \mid 2^6+1$, $(2^6-1, n^2-1)=3^2\cdot 7$ and since a Hall $\{3,7\}$-subgroup of G is cyclic, 13-rank of $G\leq \log_{13}(2^6-1+2)<2$. Thus the Sylow 13-subgroup of G is cyclic and so G is also cyclic.

Example 3. Let D be an abelian affine difference set of order $n = 2^e$ where e is an odd integer, in a group G. Clearly, $2^e + 1 \equiv 0 \pmod 3$. By Corollary 2(ii), the Sylow 3-subgroup of G is cyclic of order at least 3^{a+1}, where $3^a | e$ (cf. Theorem 6.3 of [7]). If $a > 0$ and $e < 100$, one can check that G is cyclic except in the folowing cases.

(i) $n = 2^{21}$, $G \simeq Z_9 \times Z_7 \times Z_7 \times Z_{43} \times Z_{127} \times Z_{337} \times Z_{5419}$.

(ii) $n = 2^{63}$, $G = Z_{27} \times Z_7 \times Z_7 \times C$, where C is a cyclic group.

The next result considers the case that n is an odd prime power. Under some conditions, we shall show that the rank of the Sylow 3-subgroup of G is relatively row.

Corollary 3. *Let D be an abelian affine difference set of order n in a group G. Let $n = w^e$ where w is an odd prime and e is a positive integer. Suppose $3|n+1$. Let r be the 3-rank of G. Then $r \leq \log_3(|G_{w-1}| + 2)$. Moreover, $r \leq \log_3 w$ if either* (i) $(w-1, e) = 1$ *or* (ii) *a Hall $\pi(w-1)$-subgroup of N is cyclic.*

Proof. As $3|w^e + 1$, we have $w \equiv 2 \pmod 3$ and e is odd. Hence $3|w+1$. It follows from Theorem 4 that $r \leq \log_3(|G_{w-1}| + 2)$.

Set $\pi_0 = \pi(w-1)$ and $\pi_1 = \pi(w-1) - \{2\}$. If $(w-1, e) = 1$, then $(w-1, w^{e-1} + \cdots + w + 1) = (w-1, e) = 1$ and so the Hall π_1-subgroup of G, say H, is of order $(w-1)/2^e$, where 2^e is the 2-part of $w-1$. Therefore, as the Sylow 2-subgroup of G, say P, is cyclic, we have $G_{w-1} = H \times P_{2^e}$. Hence $|G_{w-1}| = w - 1$. On the other hand, if a Hall π_0-subgroup of N is cyclic, then clearly $|G_{w-1}| = w - 1$. It follows from Theorem 4 that $r \leq \log_3(w+1)$ in both cases. If the equality holds, then $w = 3^r - 1$, which is not the case as w is an odd prime. Thus $3^r \leq w$ and so $r \leq \log_3 w$.

Example 4. Let D be an abelian affine difference set of order $n = 11^{3^b \cdot c}$ where b and c are positive integers and neither 3 nor 5 are divisors of c. We have $3^{1+b} | 11^{3^b \cdot c} + 1$, and since $(11 - 1, 3^b \cdot c) = 1$ it follows that $r \leq \log_3\{(11-1) + 2\}$. Thus $r \leq 2$. We have shown that in this case, the rank of the Sylow 3-subgroup of G is relatively low.

References

1. K.T. Arasu and A. Pott, *On quasiregular collineation groups of projective planes, Designs, Codes and Cryptography* **1** (1991), 83 - 92.

2. R.C. Bose, *An affine analogue of Singer's theorem*, J. Indian Math. Soc. **6** (1942), 1 - 15.

3. P. Dembowski and F. Piper, *Quasiregular collineation groups of finite projective planes*, Math. Zeitschrift **103** (1968), 239 - 258.

4. J.E.H. Elliot and A.T. Butson, *Relative difference sets*, Illinois J. Math. **10** (1966), 517 - 531.

5. M.J. Ganley and E. Spence, *Relative difference sets and quasiregular collineation groups*, J. Comb. Th. (A) **19** (1975), 134 - 153.

6. A.J. Hoffman, *Cyclic affine planes*, Canad. J. Math **4** (1952) 295 - 301.

7. H. Lüneburg, *Translation planes*, Springer Verlag, Berlin-Heidelberg-New York, 1980.

8. A. Pott, *Finite Geometry and character theory*, Springer, Berlin 1995.

ON ADE GROUPS IN ABELIAN GROUPS

TAKASHI OKUYAMA

All groups considered here are arbitrary abelian groups. Throughout this article, let G be an arbitrary abelian group, T be the torsion-part of G, and G_p is the p-part of G.

Fuchs has given an interesting example[1, Vol. 2 p.186 Example 2]. This group has subgroups to be almost-dense and T-high. Then this example has caused us to define almost-dense extension groups of torsion-free groups as follows:

Definition. Let A be a torsion-free group. A mixed group G is said to be an *almost-dense extension group (ADE-group)* of A if A is almost-dense and T-high of G. Such a subgroup A is called a *moho* subgroup of G.

In [2], we have considered an ADE group G of which moho subgroup is of rank 1 and of which G_p is cyclic for every prime p. In this article, we give the structure, the representation, and the realization of more generalized ADE groups G such that $r(G/T) = 1$ and G_p is a direct sum of cyclic groups for every prime p.

Structure Theorem. *Let G be an ADE group with A as a moho subgroup such that $r(A) = 1$ and G_p is a direct sum of cyclic groups for every prime p, and let $a \in A$ such that $h_p^A(a) = m_p$ for every prime p. If $m_p < \infty$, then let $a_p = \frac{1}{p^{m_p}}a$. Then, for every prime p, one of the following three cases holds.*

Case 1

(1) $G_p = \oplus_{i=1}^{\infty}\langle y_{pi}\rangle$, *where* $o(y_{pi}) = p^{t_{pi}}$ *for all* $i \geqq 1$.
(2) $(G/A)_p = \oplus_{i=1}^{\infty}\langle g_{pi} + A\rangle$, *where* $g_{pi} \in G$ *and* $o(g_{pi} + A) = p^{c_{pi}}$ *for all* $i \geqq 1$.
(3) $t_{pi} < c_{pi} < t_{pi+1}$ *for all* $i \geqq 1$.
(4) $y_{p1} = a_p + p^{c_{p1}-t_{p1}}g_{p1}$ *and* $y_{pi+1} = g_{pi} + p^{c_{pi}-t_{pi}}g_{pi+1}$ *for all* $i \geqq 1$.
(5) *For every* $i \geqq 1$, $h_p(p^k g_{pi}) = k$ *for all* $k < t_{pi+1}$.

Case 2

(1) $G_p = \oplus_{i=1}^{n_p}\langle y_{pi}\rangle$, *where* $o(y_{pi}) = p^{t_{pi}}$ *for all* $1 \leqq i \leqq n_p$.
(2) $(G/A)_p = \oplus_{i=1}^{n_p}\langle g_{pi} + A\rangle$, *where* $g_{pi} \in G$ *and* $o(g_{pi} + A) = p^{c_{pi}}$ *for all* $1 \leqq i \leqq n_p$.
(3) $t_{p1} < c_{p1} < t_{p2} < c_{p2} < t_{p3} < \cdots < c_{pn_p-1} < t_{pn_p} < c_{pn_p}$.
(4) $y_{p1} = a_p + p^{c_{p1}-t_{p1}}g_{p1}$ *and* $y_{pi+1} = g_{pi} + p^{c_{pi}-t_{pi}}g_{pi+1}$ *for all* $1 \leqq i \leqq n_p$.
(5) *For every* $1 \leqq i \leqq n_p - 1$, $h_p(p^k g_{pi}) = k$ *for all* $k < t_{pi+1}$ *and* $h_p(p^k g_{pn_p}) = k$ *for all* $k < c_{pn_p}$.

Case 3

(1) $G_p = \oplus_{i=1}^{n_p}\langle y_{pi}\rangle \oplus \langle y_p\rangle$, *where* $o(y_{pi}) = p^{t_{pi}}$ *for all* $1 \leqq i \leqq n_p$ *and* $o(y_p) = p^{t_p}$.

(2) $(G/A)_p = \oplus_{i=1}^{n_p}\langle g_{pi}+A\rangle \oplus D_p/A$, *where* $g_{pi} \in G$ *and* $o(g_{pi}+A) = p^{c_{pi}}$ *for all* $1 \leqq i \leqq n_p$, *and* D_p/A *is divisible of rank one such that*

$$D_p/A = \langle d_{pj}+A \mid pd_{pj+1} = d_{pj}, pd_{p1} \in A, j = 1,2,\dots\rangle$$

and $d_{p1}+A = p^{t_p-1}y_p$.

(3) $t_{p1} < c_{p1} < t_{p2} < c_{p2} < t_{p3} < \cdots < c_{pn_p-1} < t_{pn_p} < c_{pn_p} < t_p$.

(4) $y_{p1} = a_p + p^{c_{p1}-t_{p1}}g_{p1}, y_{pi+1} = g_{pi} + p^{c_{pi}-t_{pi}}g_{pi+1}$ *for all* $1 \leqq i \leqq n_p - 1$, *and* $y_p = g_{pn_p} + pd_{pt_p}$.

(5) *For every* $1 \leqq i \leqq n_p - 1$, $h_p(p^k g_{pi}) = k$ *for all* $k < t_{pi+1}$ *and* $h_p(p^k g_{pn_p}) = k$ *for all* $k < t_p$.■

A moho subgroup A of G is torsion-free of rank one. Hence A has a type. We define the *moho system* of G as a representative of the type of A. It is denoted by $\mathrm{M}^A(G)$. Let $A = Ra$, where p_n are all primes and R is a subgroup of $\mathbf{Q}$ generated by all $p_n^{-l_n}$ such that $l_n \leqq m_n$ and $\chi(a) = (m_1, m_2, \dots)$. Let $\mathrm{M}^A(G) = \chi(a)$. If we describe a generator a of A precisely, then we denote $\mathrm{M}^a(G)$. It is described by a sequence of nonnegative integers and ∞. We define the p-coordinate of the *QT-matrix*, denoted by $\mathbf{QT}_p^A(G)$, as follows:

$$\mathbf{QT}_p^A(G) = \begin{pmatrix} c_{p1}, c_{p2}, \dots, c_{pn}, & \cdots \\ t_{p1}, t_{p2}, \dots, t_{pn}, & \cdots \end{pmatrix}, \tag{1}$$

if G_p is in Case 1,

$$\mathbf{QT}_p^A(G) = \begin{pmatrix} c_{p1}, c_{p2}, \dots, c_{pn_p} \\ t_{p1}, t_{p2}, \dots, t_{pn_p} \end{pmatrix}, \tag{2}$$

if G_p is in Case 2,

$$\mathbf{QT}_p^A(G) = \begin{pmatrix} c_{p1}, c_{p2}, \dots, c_{pn_p}, \infty \\ t_{p1}, t_{p2}, \dots, t_{pn_p}, t_p \end{pmatrix}, \tag{3}$$

if G_p is in Case 3, and

$$\mathbf{QT}_p^A(G) = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \tag{4}$$

if $G_p = 0$. Hence such an ADE group G is determined by the moho system and the QT-matices.

Realization Theorem. *Let* $\mathrm{M} = (m_2, m_3, \dots, m_p, \dots)$, *where* m_p *is either non-negative integer or* ∞ *for all prime* p. *For every prime* p, *let* $\mathbf{QT}_p$ *be a matrix (1), where* $t_{pi} < c_{pi} < t_{pi+1}$ *for all* $i \geqq 1$ *and* $m_p < \infty$, *or* $\mathbf{QT}_p$ *be a matrix (2), where* $t_{p1} < c_{p1} < t_{p2} < c_{p2} < t_{p3} < \cdots < c_{pn_p-1} < t_{pn_p} < c_{pn_p}$ *and* $m_p < \infty$, *or* $\mathbf{QT}_p$ *be a matrix (3), where* $t_{p1} < c_{p1} < t_{p2} < c_{p2} < t_{p3} < \cdots < c_{pn_p-1} < t_{pn_p} < c_{pn_p} < t_p$ *and* $m_p < \infty$, *or* $\mathbf{QT}_p$ *be a matrix (4). Let* A *be a torsion-free group of rank* 1 *such that* M *is a representative of the type* A. *Then there exists an ADE group* G *with* A *as a moho subgroup and with* $\mathbf{QT}_p$ *as the p-coordinate of the QT-matrix for every prime* p.■

Example. For every prime p, let

$$T_p = \oplus_{i=1}^{\infty}\langle y_{pi}\rangle,$$

where $o(y_{pi}) = p^{2i}$ and define

$$\mathbf{b}_{pi} = (0,\dots,0,y_{pi},py_{pi+1},p^2y_{pi+2},\dots) \in \Pi_{i=1}^{\infty}\langle y_{pi}\rangle$$

for every prime p and $i = 1,2,\dots$. Moreover, define

$$a = (\mathbf{b}_{21},\mathbf{b}_{31},\dots,\mathbf{b}_{p1},\dots) \in \Pi_p(\Pi_{i=1}^{\infty}\langle y_{pi}\rangle)$$

and

$$g_{pj} = (\mathbf{b}_{21}^{j-1},\mathbf{b}_{31}^{j-1},\dots,\mathbf{b}_{pj},\dots) \in \Pi_p(\Pi_{i=1}^{\infty}\langle y_{pi}\rangle),$$

where $p\mathbf{b}_{q1}^{j-1} = \mathbf{b}_{q1}^{j-2}$ and $\mathbf{b}_{q1}^{0} = \mathbf{b}_{q1}$ for every $q \neq p$ and $j = 2,3,4,\dots$. Then $a = g_{p1}$ for every prime p. Let $T = \oplus_p T_p$ and

$$G = \langle T, g_{pj} | j = 1,2\dots\rangle.$$

Then T becomes the torsion part of G and G is an ADE group of rank 1 with A as a moho subgroup. G also has $(0,\dots,0,\dots)$ as a moho system and the following matrix as the p-cordinate of the QT-matrices:

$$\mathbf{QT}_p^A(G) = \begin{pmatrix} 3 & 5 & 7 & 9 & \dots \\ 2 & 4 & 6 & 8 & \dots \end{pmatrix}.$$

Standing Assumptions. *Let G be an ADE group with A as a moho subgroup such that $r(A) = 1$ and G_p is a direct sum of cyclic groups for every prime p. Moreover, G has either matix (1) or (2) or (3) or (4) as the* **QT***-matrix of the p-coordinate for every prime p, and let $a \in A$ such that $\mathbf{M}_p^a(G) = m_p$. Let $a_p = \frac{1}{p^{m_p}}a \in A$ if $m_p < \infty, t_{pn_p+1} = t_p$, and for every p and $i \geqq 1$, g_{pi} and y_{pi} be the ones as mentioned in the structure theorem in the former article "On ADE groups of rank one 1".*

From now on, let G be a group satisfying Standing Assumption if we do not give special references. Our goal is to classify ADE groups G satisfying Standing Assumption.

Definition. Then, for every prime p, let

$$e_{pn}^A(G) = \begin{cases} 0 & \text{for } n = 0 \\ t_{p1} & \text{for } n = 1 \\ t_{p1} + \Sigma_{i=2}^{n}(t_{pi} - c_{pi-1}) & \text{for } n \geqq 2 \text{ if } t_{pn} \neq 0. \end{cases}$$

$e_{pn}^A(G)$ is called the *nth elevation* of G under a moho subgroup A. Let $a \in A$. If n is the largest integer such that $h_p^A(a) \geqq e_{pn}^A(G)$, then it is said that a has *nth elevation at p* and we denote $e_p(a) = n$.

We consider that if $G_p = 0$, then $e_{p0}^A(G) = 0$. By [2, Proposition 2.2(2)], if $h_p^A(a) = \infty$, then $G_p = 0$. Hence we have $e_p(a) = 0$ and it is well defined. The elevations play a pivote role in changing the configuration of these ADE groups. Moreover, let

$$\mathfrak{P}^a(G) = \{p \in \mathfrak{P}(G) | m_p \geqq t_{p1}\}.$$

We call the top row of the QT-matrices the p-coordinate of the *quotient system*, denoted by $\mathbf{Q}_p^A(G)$. Moreover, $\mathbf{Q}_{pi}^A(G)$ means the ith coordinate of $\mathbf{Q}_p^A(G)$ at the prime p, that is $\mathbf{Q}_{pi}^A(G) = c_{pi}$ and define

$$|\mathbf{Q}_p^{A_1}(G_1) - \mathbf{Q}_p^{A_2}(G_2)| = \Sigma_p |c_{pi}^1 - c_{pi}^2|,$$

where $\mathbf{Q}_p^{A_i}(G_i) = (c_{pj}^i), i = 1, 2, j = 1, 2, \ldots$.

Classification Theorem. *For $i = 1, 2$, let G_i be an ADE group with A_i as a moho subgroups such that $r(A_i) = 1$ and $(G_i)_p$ is a direct sum of cyclic groups for every prime p. Then $G_1 \cong G_2$ if and only if there exists a generator a_i of A_i for $i = 1, 2$ such that*

(1) $T(G_1) \cong T(G_2)$,
(2) *for every prime p, $e_p(a_1) = e_p(a_2) = r_p$,*
(3) $\Sigma_{p \in \mathfrak{P}^{a1}(G_1)} |\mathbf{Q}_p^{A_1}(G_1) - \mathbf{Q}_p^{A_2}(G_2)| < \infty$ *and*
$\Sigma_{p \in \mathfrak{P}^{a1}(G_1)} |\mathbf{M}_p^{A_1}(G_1) - \mathbf{M}_p^{A_2}(G_2)| < \infty$ *[if we set $\infty - \infty = 0$], and*
(4)

$$\Sigma_{p \in \mathfrak{P}^{a1}(G_1)} \{\Sigma_{i \leqq r_p} |(\mathbf{M}_p^{A_1}(G_1) + \Sigma_{i=1}^{r_p} \mathbf{Q}_{pi}^{A_1}(G_1)) - (\mathbf{M}_p^{A_2}(G_2) + \Sigma_{i=1}^{r_p} \mathbf{Q}_{pi}^{A_2}(G_2))|)\} < \infty$$

$\Sigma_{p \in \mathfrak{P}^{a1}(G_1), i > r_p} |\mathbf{Q}_{pi}^{A_1}(G_1) - \mathbf{Q}_{pi}^{A_2}(G_2)| < \infty$, *and*
$\Sigma_{p \in \mathfrak{P}^{a1}(G_1), i > r_p} |\mathbf{M}_p^{A_1}(G_1) - \mathbf{M}_p^{A_2}(G_2)| < \infty$. *[if we set $\infty - \infty = 0$].*■

In general, let G be an ADE group. If T is bounded, then G is splitting. However, the ADE group G mentioned in Example in the section 1 in [1] is not splitting. Then we can pose the problem: Which ADE group splits ?

Now we give a necessary and sufficient condition for an group G satisfying Standing Assumption to be splitting.

Splitting Theorem. *G is splitting if and only if*

(1) *there exists no prime p such that $\oplus_{i=1}^{\infty} \langle y_{pi} \rangle$ and*
(2) *there exists a generator $a \in A$ such that*

$$e_p(a) \geqq \begin{cases} n_p & \text{if } \oplus_{i=1}^{n_p} \langle y_{pi} \rangle \\ n_p + 1 & \text{if } \oplus_{i=1}^{n_p} \langle y_{pi} \rangle \oplus \langle y_p \rangle. \blacksquare \end{cases}$$

Corollary 1. *If G_p is not bounded for some prime p, then there exists no T-high subgroup that is purifiable in G.*■

Not all moho subgroups of an ADE group G satisfying Standing Assumption are isomorphic. Then we characterize a group G that all moho subgroups of G are isomorphic as follows:

Theorem 2. *All moho subgroups of G are isomorphic if and only if, either*

(1) *G is basic or*
(2) *for almost all $p \in \mathfrak{P}^A(G)$, $c_{p1} = t_{p1} + 1$ and $m_p = t_{p1}$.*■

REFERENCES

1. L.Fuchs, *Infinite Abelian Groups I,II*, Academic Press, New York, 1970, 1973.
2. T.Okuyama, *On Almost-Dense Extension Groups of Torsion-Free Groups*, J.Algebra 202 (1998), 202-228..
3. ———, *On Almost-Dense Extension Groups of Torsion-Free Groups*, J.Algebra 202 (1998), 202-228..

DEPARTMENT OF MATHEMATICS, TOBA NATIONAL COLLEGE OF MARITIME TECHNOLOGY, 1-1, IKEGAMI-CHO, TOBA-SHI, MIE-KEN, 517, JAPAN.
E-mail address: okuyamat@toba-cmt.ac.jp

On Singleton bounds for codes over Z_4

Keisuke SHIROMOTO

Department of Mathematics, Kumamoto University,
2-39-1. Kurokami, Kumamoto 860-0862, JAPAN:
keisuke@math.sci.kumamoto-u.ac.jp

1 Introduction

Let $R := Z_4 = \{0, 1, 2, 3\}$ be a ring of 4-elements and $V := R^n$ be the free module of rank n consisting of all n-tuples of elements of R. A code C of length n over R is an additive subgroup of V. We note that C is also an R-submodule of V. An element of C is called a codeword of C. Codes differing by only a permutation of coordinates are called permutation-equivalent. Any code is permutation-equivalent to a code C with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & X & Y \\ 0 & 2I_{k_2} & 2Z \end{pmatrix},$$

where Y is a matrix over Z_4 and X and Z are binary matrices (see [2]). The code is then an abelian group of type $4^{k_1}2^{k_2}$, containing $2^{2k_1+k_2}$ codewords. We indicate this by writing $|C| = 4^{k_1}2^{k_2}$. In this paper, we use four kinds of weights, namely the complete weight, the Hamming weight, the Lee weight and the Euclidean weight. For every $x = (x_1, \cdots, x_n) \in V$ and $r \in R$, the *complete weight* of x is defined by

$$n_r(x) := |\{i \mid x_i = r\}|.$$

Given any element $x \in V$, the *Hamming weight*, the *Lee weight* and the *Euclidean weight* of x, denoted by H-wt(x), L-wt(x) and E-wt(x), respectively, are defined by

$$\begin{aligned} \text{H-wt}(x) &:= n_1(x) + n_2(x) + n_3(x), \\ \text{L-wt}(x) &:= n_1(x) + 2n_2(x) + n_3(x), \\ \text{E-wt}(x) &:= n_1(x) + 4n_2(x) + n_3(x). \end{aligned}$$

Put $N = \{1, 2, \cdots, n\}$. We define the *supports* of Hamming type, Lee type and Euclidean type of a vector $x = (x_1, \cdots, x_n) \in V$, denoted by $\mathrm{supp}_H(x)$, $\mathrm{supp}_L(x)$, $\mathrm{supp}_E(x)$, respectively, by

$$\begin{aligned}
\mathrm{supp}_H(x) &:= \{i \in N \mid x_i \neq 0\}, \\
\mathrm{supp}_L(x) &:= \{i \in N \mid x_i = 1, 3\} \cup \{j, j \mid x_j = 2, j \in N\}, \\
\mathrm{supp}_E(x) &:= \{i \in N \mid x_i = 1, 3\} \cup \{j, j, j, j \mid x_j = 2, j \in N\},
\end{aligned}$$

where $\mathrm{supp}_L(x)$ and $\mathrm{supp}_E(x)$ are viewed as multi-sets. Clearly, we have that $|\mathrm{supp}_H(x)| = |\text{H-wt}(x)|$, $|\mathrm{supp}_L(x)| = |\text{L-wt}(x)|$ and $|\mathrm{supp}_E(x)| = |\text{E-wt}(x)|$. The minimum Hamming, Lee and Euclidean weights of C, denoted by d_H, d_L and d_E, respectively, are the smallest weights among all non-zero codewords of C. The inner product of vectors $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$ is defined by

$$\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n \pmod 4.$$

The dual code of C is defined by

$$C^{\perp} := \{y \in V \mid \langle x, y \rangle = 0 \quad (\forall x \in C)\}.$$

The following proposition is well-known as the Singleton bound (see [7]).

Proposition 1 *Let C be a q-array (not necessary linear) $[n, M, d]$-code, where $M = |C|$. Then.*

$$M \leq q^{n-d+1}$$

The main purpose of this paper is to give an another proof of the above bound for d_H over Z_4 and find the similar type bounds for d_L and d_E over Z_4.

2 Another proof of Singleton bound for Hamming weight

In this section, we prove the Singleton bound for Hamming weight over Z_4 by using the algebraic methods. For a submodule D of V and a subset $M \subseteq N = \{1, 2, \cdots, n\}$, let

$$\begin{aligned}
D(M) &:= \{x \in D \mid \mathrm{supp}_H(x) \subseteq M\}, \\
D^* &:= \mathrm{Hom}_R(D, R).
\end{aligned}$$

Clearly $D(M) = D \cap V(M)$ is a submodule of V and $|V(M)| = 4^{|M|}$. By the fundamental theorem of finite abelian groups, we have that $|D| = |D^*|$ for any submodule of V. The following lemma (there is a similar result over $GF(q)$ in [10]) is essential.

Lemma 1 *Let C be a code over Z_4 and $M \subseteq N$. Then there is an exact sequence as R-modules:*

$$0 \longrightarrow C^{\perp}(M) \xrightarrow{\text{inc}} V(M) \xrightarrow{f} C^{*} \xrightarrow{\text{res}} C(N-M)^{*} \longrightarrow 0,$$

where the maps inc, res *denote the inclusion map, the restriction map, respectively, and the map f is defined by*

$$f : y \longmapsto (\hat{y} : x \mapsto \langle x, y \rangle).$$

Proof. Clearly the map *inc* is injective. Since Z_4 is a self-injective module over itself, the map *res* is surjective. If we take a codeword $y \in C^{\perp}(M)$, then

$$\hat{y} : x \mapsto \langle x, y \rangle = 0 \quad (\forall x \in C),$$

and so $y \in \ker f$, which implies

$$\text{Im(inc)} \subseteq \ker f.$$

Conversely, if we take an element $y \in \ker f$, that is, $\hat{y} = 0$, then

$$y \in V(M) \cap C^{\perp} = C^{\perp}(M),$$

and so

$$\text{Im(inc)} \supseteq \ker f.$$

Thus we have

$$\text{Im(inc)} = \ker f.$$

Next if we take a codeword $y \in V(M)$, then

$$\hat{y} : x \mapsto \langle x, y \rangle = 0 \quad (\forall x \in C(N-M)),$$

and so $y \in \ker(\text{res})$, which shows that

$$\text{Im}f \subseteq \ker(\text{res}).$$

Conversely, if $\lambda \in \ker(\text{res})$, then

$$\lambda(x) = 0 \quad (\forall x \in C(N-M)),$$

and there exists $y \in V$ with $\lambda = \hat{y}$. (Note that $V \longrightarrow C^{*} : v \mapsto \hat{v}$ is surjective.) So $\langle x, y \rangle = 0$, that is,

$$\begin{aligned} y &\in (C(N-M))^{\perp} = (C \cap V(N-M))^{\perp} \\ &= C^{\perp} + V(N-M)^{\perp} = C^{\perp} + V(M). \end{aligned}$$

Since $\hat{z} = 0$ for any $z \in C^{\perp}$, we have

$$\mathrm{Im}f \supseteq \ker(\mathrm{res}).$$

Thus

$$\mathrm{Im}f = \ker(\mathrm{res}).$$

Hence the lemma follows. ∎

We remark that we can prove the MacWilliams identity for codes over Z_4 ([6]) by using Lemma 1 (there are similar results over $GF(q)$ in [8] and [10]).

Using the above lemma, we prove the following proposition.

Proposition 2 *Let C be a code of length n over Z_4 with $|C| = 4^{k_1}2^{k_2}$ and the minimum Hamming weight d_H. Then*

$$2d_H \leq 2n - 2k_1 - k_2 + 2.$$

Proof. By Lemma 1, we have

$$|C| \cdot |C^{\perp}(N - \widetilde{M})| = |V(N - \widetilde{M})| \cdot |C(\widetilde{M})|,$$

where $\widetilde{M} = N - M$. If we take a subset M of N with $|\widetilde{M}| = d_H - 1$, then $|C(\widetilde{M})| = 1$ and $|C^{\perp}(N - \widetilde{M})| \geq 1$. Thus we have the following inequality:

$$4^{k_1}2^{k_2} \leq 4^{n-(d_H-1)}.$$

Hence the proposition follows. ∎

Example. Let C be the code over Z_4 with the generator matrix

$$G = \left(\begin{array}{cc} I_{n-1} & \mathbf{1}^t \end{array} \right),$$

where $\mathbf{1}$ is the all-one row vector. Then, C is a code with the equality in the above theorem, since $k_1 = n - 1$, $k_2 = 0$ and $d_H = 2$.

Recently, K.Shiromoto and T.Yoshida([9]) prove the stronger Singleton type bound than Theorem 1 as follows;

Theorem 1 (Shiromoto and Yoshida) *Let C be a code of length n over Z_4 with $|C| = 4^{k_1}2^{k_2}$ and the minimum Hamming weight d_H. Then*

$$d_H \leq n - k_1 - k_2 + 1.$$

3 Singleton bounds for other weights

We also can get the similar results for d_L, d_E. Now we give the similar definitions and notation. For any subset $M = \{i_1, i_2, \cdots, i_m\} \subseteq N$, M_2, M_4 denote the multi-sets such that

$$\begin{aligned} M_2 &= \{i_1, i_1, i_2, i_2, \cdots\cdots, i_m, i_m\}, \\ M_4 &= \{i_1, i_1, i_1, i_1, i_2, i_2, i_2, i_2, \cdots\cdots, i_m, i_m, i_m, i_m\}. \end{aligned}$$

For a submodule D of V and a subset $M \subseteq N = \{1, 2, \cdots, n\}$, let

$$\begin{aligned} D(M_2) &:= \{x \in D \mid \mathrm{supp}_L(x) \subseteq M_2\}, \\ D(M_4) &:= \{x \in D \mid \mathrm{supp}_E(x) \subseteq M_4\}. \end{aligned}$$

Clearly $D(M_2) = D \cap V(M_2)$ and $D(M_4) = D \cap V(M_4)$ are submodules of V and $|V(M_2)| = |V(M_4)| = 4^{|M|}$. Under the above notation, the following two lemmas also can be proved by the same way as Lemma 2, so the proofs are omitted.

Lemma 2 *Let C be a code over Z_4 and $M \subseteq N$. Then there is an exact sequence as R-modules:*

$$0 \longrightarrow C^{\perp}(M_2) \xrightarrow{\mathrm{inc}} V(M_2) \xrightarrow{f} C^{*} \xrightarrow{\mathrm{res}} C(N_2 - M_2)^{*} \longrightarrow 0.$$

Lemma 3 *Let C be a code over Z_4 and $M \subseteq N$. Then there is an exact sequence as R-modules:*

$$0 \longrightarrow C^{\perp}(M_4) \xrightarrow{\mathrm{inc}} V(M_4) \xrightarrow{f} C^{*} \xrightarrow{\mathrm{res}} C(N_4 - M_4)^{*} \longrightarrow 0.$$

Using the above lemmas, we have the following theorems.

Theorem 2 *Let C be a code of length n over Z_4 with $|C| = 4^{k_1}2^{k_2}$ and the minimum Lee weight d_L. Then*

$$2\left[\frac{d_L - 1}{2}\right] \leq 2n - 2k_1 - k_2.$$

Proof. By Lemma 2, we have

$$|C| \cdot |C^{\perp}(N_2 - \widetilde{M_2})| = |V(N_2 - \widetilde{M_2})| \cdot |C(\widetilde{M_2})|,$$

where $\widetilde{M_2} = N_2 - M_2$. If we take a subset M of N with $|\widetilde{M_2}| = 2\left[\frac{d_L - 1}{2}\right]$, where $[a] := \mathrm{Max}\{m \in Z | m \leq a\}$, then $|C(\widetilde{M_2})| = 1$ and $|C^{\perp}(N_2 - \widetilde{M_2})| \geq 1$. Thus we have the following inequality:

$$4^{k_1}2^{k_2} \leq 4^{n - \left[\frac{d_L - 1}{2}\right]}.$$

Hence the theorem follows. ∎

The Gray map $\phi : Z_4 \to Z_2^2$ is defined by $\phi(0) = 00$, $\phi(1) = 01$, $\phi(2) = 11$, and $\phi(3) = 10$. It is well-known that ϕ is a distance-preserving map from (Z_4^n , Lee distance) to (Z_2^{2n} , Hamming distance) (see [5]). Using Theorem 2, we have the Singleton bound for some binary nonlinear codes.

Corollary 1 *If a binary nonlinear $(2n, M, d)$-code B, where $M := |B|$, is the Gray map image of a code over Z_4, then*

$$2\left[\frac{d-1}{2}\right] \leq 4n - \log_2 M.$$

We now prove the Singleton bound with respect to Euclidean weight.

Theorem 3 *Let C be a code of length n over Z_4 with $|C| = 4^{k_1}2^{k_2}$ and the minimum Euclidean weight d_E. Then*

$$2\left[\frac{d_E - 1}{4}\right] \leq 2n - 2k_1 - k_2.$$

For convenience, we give the proof of Theorem 3, though that is similar to the proof of Theorem 2.

Proof. By Lemma 3, we have

$$|C| \cdot |C^{\perp}(N_4 - \widetilde{M_4})| = |V(N_4 - \widetilde{M_4})| \cdot |C(\widetilde{M_4})|,$$

where $\widetilde{M_4} = N_4 - M_4$. If we take a subset M of N with $|\widetilde{M_4}| = 4\left[\frac{d_E-1}{4}\right]$, then $|C(\widetilde{M_4})| = 1$ and $|C^{\perp}(N_4 - \widetilde{M_4})| \geq 1$. Thus we have the following inequality:

$$4^{k_1}2^{k_2} \leq 4^{n-\left[\frac{d_E-1}{4}\right]}.$$

Hence the theorem follows. ∎

4 An application to codes over Z_l

We can prove the Singleton bounds for codes over Z_l as well as codes over Z_4. Naturally, we can define the Lee weight and the Euclidean weight as follows. In the case of $l = 2k$, the Lee weights and the Euclidean weights of the elements $0, \pm 1, \pm 2, \pm 3, \cdots, \pm(k-1), k$ of Z_l are defined by $0, 1, 2, 3, \cdots, (k-1), k$ and $0, 1, 4, 9, \cdots, (k-1)^2, k^2$, respectively. In the case of $l = 2k+1$, the Lee weights and the Euclidean weights of the elements $0, \pm 1, \pm 2, \pm 3, \cdots, \pm(k-1), \pm k$ of Z_l are defined by $0, 1, 2, 3, \cdots, (k-1), k$ and $0, 1, 4, 9, \cdots, (k-1)^2, k^2$, respectively. The Lee weight and The Euclidean weight of a vector are the rational sum of the Lee weights and the Euclidean weights of its components respectively. The Hamming weight of a vector is the number of non-zero components in the vector. We define the supports of Lee type and Euclidean type of a vectors $x = (x_1, \cdots, x_n) \in Z_l^n$ by

$$\mathrm{supp}_L(x) := \begin{cases} \{i_1 \in N \mid x_{i_1} = \pm 1\} \cup \{i_2, i_2 \mid x_{i_2} = \pm 2, i_2 \in N\} \cup \cdots \cup \overbrace{\{i_k, i_k, \cdots, i_k}^{k \text{ times}} \\ \mid x_{i_k} = k, i_k \in N\} \qquad (\text{if } l = 2k) \\ \{i_1 \in N \mid x_{i_1} = \pm 1\} \cup \{i_2, i_2 \mid x_{i_2} = \pm 2, i_2 \in N\} \cup \cdots \cup \overbrace{\{i_k, i_k, \cdots, i_k}^{k \text{ times}} \\ \mid x_{i_k} = \pm k, i_k \in N\} \qquad (\text{if } l = 2k+1), \end{cases}$$

$$\mathrm{supp}_E(x) := \begin{cases} \{i_1 \in N \mid x_{i_1} = \pm 1, \} \cup \{i_2, i_2, i_2, i_2 \mid x_{i_2} = \pm 2, i_2 \in N\} \cup \cdots \cup \overbrace{\{i_k, i_k, \cdots, i_k}^{k^2 \text{ times}} \\ \mid x_{i_k} = k, i_k \in N\} \qquad (\text{if } l = 2k) \\ \{i_1 \in N \mid x_{i_1} = \pm 1, \} \cup \{i_2, i_2, i_2, i_2 \mid x_{i_2} = \pm 2, i_2 \in N\} \cup \cdots \cup \overbrace{\{i_k, i_k, \cdots, i_k}^{k^2 \text{ times}} \\ \mid x_{i_k} = \pm k, i_k \in N\} \qquad (\text{if } l = 2k+1), \end{cases}$$

where $\mathrm{supp}_L(x)$ and $\mathrm{supp}_E(x)$ are viewed as multi-sets. Similar arguments to Theorem 2 and Theorem 3 show the following results, so the proofs are omitted.

Corollary 2 *Let C be a code of length n over Z_l with the minimum Lee weight d_L and the minimum Euclidean weight d_E. Then*

$$\begin{cases} \left[\frac{d_L - 1}{k}\right] \le n - \log_{2k} |C| & (\text{if } l = 2k) \\ \left[\frac{d_L - 1}{k}\right] \le n - \log_{2k+1} |C| & (\text{if } l = 2k+1) \end{cases} \quad \textit{and}$$

$$\begin{cases} \left[\frac{d_E - 1}{k^2}\right] \le n - \log_{2k} |C| & (\text{if } l = 2k) \\ \left[\frac{d_E - 1}{k^2}\right] \le n - \log_{2k+1} |C| & (\text{if } l = 2k+1) \end{cases}$$

Acknowledgment: The author would like to thank adviser Professor Tomoyuki Yoshida for his helpful suggestions and Dr Masaaki Harada for his helpful comments on codes over Z_4.

References

[1] E. R. Berlekamp, *Algebraic coding theory*, MaGrow-Hill, Series in Systems Science, 1970.

[2] J. H. Conway and N. J. A. Sloane, Self-dual codes over the integers Modulo 4, *Journal of Combinatorial Theory* A 62, 30–45 (1993).

[3] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, New York: Interscience Publishers, 1962.

[4] S. T. Dougherty, M. Harada and P. Solé, Shadow codes over Z_4, 1997, preprint.

[5] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, The Z_4 -linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE trans. Inform. Theory*, Vol. 40, 301–319 (1994).

[6] M. Klemm, Über die identität von MacWilliams für die gewichtsfunktion von codes, *Arch. Math.*, Vol. 49, 400–406 (1987).

[7] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, Amsterdam: North Holland, 1977.

[8] K. Shiromoto, A new MacWilliams type identity for linear codes, *Hokkaido Math. J.*, 25 (1996), 651–656.

[9] K. Shiromoto and T. Yoshida, A Singleton bound for linear codes over Z/lZ, 1998, preprint.

[10] T. Yoshida, MacWilliams identities for linear codes with group action, *Kumamoto Math. J.*, 6 (1993), 29–45.

The Complex Leech Lattice and the Suzuki Group

北詰 正顕

千葉大 理学部 数学・情報数理学科

本稿では，Complex Leech Lattice から出発して，Monster と VOA に関連して調べたい・考えたいと思っていることについて報告する。新しい結果というものは含まれていないことをあらかじめご了承願いたい。

1 Complex Leech Lattice

まず，Complex Leech lattice を定義しよう。

はじめに，記号 G_{12} で ternary Golay code を表す。すなわち，G_{12} は長さ 12 の 3 元体上の符号（12 次元ベクトル空間 $\mathbf{F}_3^{12}$ の部分空間）で，次の生成行列で定義される（その列ベクトルで生成される）ものとする。

$$\left\{\begin{array}{cccccccccccc} 0&0&0&0&0&0&1&1&1&1&1&1\\ 1&0&0&0&0&2&0&1&2&2&1&0\\ 0&1&0&0&0&2&1&0&1&2&2&0\\ 0&0&1&0&0&2&2&1&0&1&2&0\\ 0&0&0&1&0&2&2&2&1&0&1&0\\ 0&0&0&0&1&2&1&2&2&1&0&0 \end{array}\right\}$$

通常は生成行列の左側に単位行列が現れるようにするのであるが，後での話で記号が見やすくなるようにしてある。１２番目の成分を一番前に並べ替えれば標準的なものになる。なお，上記の 6 つのベクトルの総和は $(1,1,1,1,1,1,1,1,1,1,1,1)$ になり，従って，$(1,1,1,1,1,1,0,0,0,0,0,0)$ も G_{12} に属する。

次に，$\mathbf{Z}[\omega]$ 上の lattice Γ_{12} を次の式で定義する。ここで，ω は 1 の原始 3 乗根で，$\theta=\sqrt{-3}$ とおく。また，G_{12} の成分を整数と見なしたベクトル全体を $\tilde{G}_{12}$ で表し，さらに記号 $\mathbf{0},\mathbf{1},\mathbf{2}$ で成分がすべて等しい（それぞれ $0,1,2$ の）ベクトルを表すことにする。

$$\Lambda=\left\{\begin{array}{l|cc} \mathbf{0}+\theta c+3x & & \Sigma x_i\equiv 0 \pmod\theta\\ \mathbf{1}+\theta c+3y & c\in\tilde{G}_{12} & \Sigma y_i\equiv 1 \pmod\theta\\ \mathbf{2}+\theta c+3z & x,y,z\in\mathbf{Z}[\omega]^{12}, & \Sigma z_i\equiv 2 \pmod\theta \end{array}\right\}$$

ここでは，通常のユニタリ計量を考えることとし，各ベクトルの長さの平方をベクトルのノルムと呼ぶことにしよう。すると，Γ_{12} の元のノルムは9の倍数になり，零ベクトルを除いた最小ノルムは18になる。そこで，長さ $9n$ のベクトル全体を $\Gamma_{12}(n)$ と表すことにする。重要なのは $n=2,3$ のときであるが，特に $\Gamma_{12}(2)$ の元をいくつか書いておこう。

$$(\theta^6,0^6),(3,-3,0^{10}),(2-\theta,\omega^5,1^6),((-2)^2,1^{10})$$

ただし，θ^6 と書いてあるのは θ が6カ所にあるという意味である。群論でよく知られる事実は，この自己同型群 $\mathrm{Aut}(\Gamma_{12})$ が散在型の鈴木単純群を位数6の中心で拡大した群になっているということである。すなわち

$$\mathrm{Aut}(\Gamma_{12}) \cong 6\cdot Suz$$

次に $\Gamma_{12}/\theta\Gamma_{12}$ について述べる。まず加群としては

$$\Gamma_{12}/\theta\Gamma_{12} \cong \mathbf{F}_3^{12}$$

が成り立つ。このとき，$\mod \theta\Gamma_{12}$ での代表元は零ベクトルと $\Gamma_{12}(2)\cup\Gamma_{12}(3)$ からとれることが知られている。また，ここには次によって内積が定義される。

$$(\bar{x},\bar{y}) := \frac{1}{3\theta}(x,y) \mod \theta$$

これはシンプレクティックな計量（すなわち $(\bar{x},\bar{x})=0$ が成り立つ）になる。ひとつの素朴な疑問は，この空間の極大全等方部分空間 W をとるとき，その全逆像 Γ_W は Γ_{12} のどのような sublattice になっているだろうか，というものである。

ここでは，現れる sublattice のひとつの（多分，最も興味深い）例を挙げよう。すべてを分類することも可能であろうが，私の怠慢もあって調べていない。ランクが小さいから，現れうる候補も数少ないはずである。たとえば，E_6, E_8 型のルートラティスを complex lattice と見なしたもの（それぞれ rank 3, 4）が出てくるであろう。

ここでの1例というのは，次で生成されるものである。

$$\begin{array}{ll}
(\theta,\theta,\theta,\theta,\theta,\theta,0,0,0,0,0,0) & (0,0,0,0,0,0,\theta,\theta,\theta,\theta,\theta,\theta)\\
(3,-3,0,0,0,0,0,0,0,0,0,0) & (0,0,0,0,0,0,3,-3,0,0,0,0)\\
(0,3,-3,0,0,0,0,0,0,0,0,0) & (0,0,0,0,0,0,0,3,-3,0,0,0)\\
(0,0,3,-3,0,0,0,0,0,0,0,0) & (0,0,0,0,0,0,0,0,3,-3,0,0)\\
(0,0,0,3,-3,0,0,0,0,0,0,0) & (0,0,0,0,0,0,0,0,0,3,-3,0)\\
(0,0,0,0,3,-3,0,0,0,0,0,0) & (0,0,0,0,0,0,0,0,0,0,3,-3)
\end{array}$$

これはよく知られた Coxeter-Todd lattice の2つの直和と同型になっている。Coxeter-Todd の定義はしないが，上記のベクトルの前半の6つの成分で生成されるもの，というのが定義そのものである。

全自己同型群における sublattice の固定部分群は 3-local 極大部分群になっていて，鈴木群の中では $3\cdot\Omega^-(6,3).2$ という形をしている。また，$\Gamma_{12}(2)$ に属するベクトルに関する complex reflection が，この部分群を生成している。

さて，こうした状況を散在型単純群 Monster M の中で観察することができる。M の位数3の元の共役類は2つあるが，それを ATLAS の記法で $3A, 3B$ と書くことにすると，$3B$ の元の中心化群に鈴木群が現れる。

$$C_{\mathrm{M}}(3B) \cong 3_{+}^{1+12}(2 \cdot Suz.2)$$

ここで 3_{+}^{1+12} は位数 3^{1+12} の plus type の extraspecial 3-group を表し，これを Q_3 とおくことにする。この群は位数3の中心を持ち，その剰余群は elementary abelian group になる。すなわち

$$Q_3/Z(Q_3) \cong \mathbf{F}_3^{12}$$

で，さらに $\bar{x} = xZ(Q_3), \bar{y} = yZ(Q_3) \in Q_3/Z(Q_3)$ に対し，

$$(\bar{x}, \bar{y}) = x^{-1}y^{-1}xy \in Q_3/Z(Q_3) \cong \mathbf{F}_3$$

により，シンプレクティック計量が定義できる。これにより鈴木群の作用を込みにして，同型

$$Q_3/Z(Q_3) \cong \Gamma_{12}/\theta\Gamma_{12}$$

が成り立つ。単位元以外については，右辺は先にふれたように $\Gamma_{12}(2) \cup \Gamma_{12}(3)$ から代表系がとれるが，これが左辺における $3A, 3B$ に対応している。

$$\begin{aligned} 3A &\longleftrightarrow \Gamma_{12}(2) \\ 3B &\longleftrightarrow \Gamma_{12}(3) \end{aligned}$$

また，内積が0になることは，Γ_{12} では直交を意味するが，Q_3 では可換を意味する。従って，Γ_{12} の sublattice の話は，Q_3 の elememtary abelian subgroup の話になる。先に掲げた Γ_W に対応する部分群を E_W とおくことにする。Γ_W の生成元がすべて $\Gamma_{12}(2)$ の元であったから，E_W は $3A$ 元で生成される。おそらく，このような Q_3 の elememtary abelian subgroup は，これに限るように思われる。

2 (Real) Leech Lattice

以上で述べたことは，Complex Leech Lattice から始めずに，通常の (Real) Leech lattice から出発して同様の議論を進めることができる。これについては，数年前の代数的組合せ論シンポジウムでお話ししているのであるが，ここでざっとおさらいをしてみよう。

Γ_{24} で Leech lattice を表すことにする。すなわち，24次元の even unimodular lattice でノルム2の元（ルートと呼ぶ）を含まないものである。ルートを含むものの分類もできていて同型を除いて2 3個存在する。これらを総称して Niemeier lattice と呼ぶ。Leech lattice のノルム $2n$ のベクトル全体を $\Gamma_{24}(n)$ と表す。$\Gamma_{24}(1) = \emptyset$ である。

Γ_{24} の自己同型群として Conway 群が現れる。

$$\mathrm{Aut}(\Gamma_{24}) \cong 2 \cdot (Co.1)$$

この群は，Monster の位数２の元（２つの共役類 $2A, 2B$ のうちの $2B$）の中心化群としても現れる。

$$C_{\mathbb{M}}(2B) \cong 2_+^{1+24} \cdot (Co.1)$$

この中心化群の正規 2-部分群 (2_+^{1+24}) を Q_2 とおく。

$Q_2/Z(Q_2)$ は $\mathbf{F}_2^{24}$ と同型になり，２次形式が $\bar{x} = xZ(Q_2) \in Q_2/Z(Q_2)$ に対し $f(\bar{x}) := x^2 \in Z(Q_2) \cong \mathbf{F}_2$ で与えられる。（標数が２なので単に計量が定義できること以上のことになっている。）

この $Q_2/Z(Q_2)$ が $Co.1-$ 加群として $\Gamma_{24}/2\Gamma_{24}$ と同型になる。

$$Q_2/Z(Q_2) \cong \Gamma_{24}/2\Gamma_{24} (\cong \mathbf{F}_2^{24})$$

右辺の代表系は $\Gamma_{24}(2) \cup \Gamma_{24}(3) \cup \Gamma_{24}(4)$ からとれるが，やはり左辺の共役類と対応している。

$$\begin{aligned} 2A &\longleftrightarrow \Gamma_{24}(2) \\ 4A &\longleftrightarrow \Gamma_{24}(3) \\ 2B &\longleftrightarrow \Gamma_{24}(4) \end{aligned}$$

ここで，全等方部分空間 W を考えれば，それは Q_2 の elementary abelian sungroup E_W と Γ_{24} の sublattice Γ_E を与える。著しい事実は，この sublattice として Niemeier lattice の $\sqrt{2}$ 倍がすべて現れるということである。たとえば，

$$\sqrt{2}(E_8 \oplus E_8 \oplus E_8), \quad \sqrt{2}\Gamma_{24}$$

は Γ_{24} の sublattice になる。前者は $\Gamma_{24}(2)$ に属する元で生成され，後者は $\Gamma_{24}(2)$ の元をいっさい含まない。従って，対応する Q_2 の部分群 E_W は，前者は $2A$ 元で生成され，後者は $2A$ 元を含まない。

3 Monster Vertex Operator Algebra

さて，ここから話は頂点作用素代数 (VOA) の話に移る。以下，用語の定義はすべて省略する。

Monster VOA を $V^\natural$ で表す。その全自己同型群が散在型単純群 Monster である。宮本雅彦氏の結果によれば Monster の位数３の元は以下のように記述することができる。

$V^\natural$ の subVOA として $S = L(\frac{4}{5}, 0) \oplus L(\frac{4}{5}, 3)$ という構造のものが存在する。この subVOA の規約加群は同型を除いて，次の６種類のいずれかに同型である。

$$L(\frac{4}{5},0) \oplus L(\frac{4}{5},3), L(\frac{4}{5},\frac{2}{5}) \oplus L(\frac{4}{5},\frac{7}{5}), L(\frac{4}{5},\frac{2}{3})^+, L(\frac{4}{5},\frac{2}{3})^-, L(\frac{4}{5},\frac{1}{15})^+, L(\frac{4}{5},\frac{1}{15})^-$$

従って，$V^\natural$ は S-加群として上記と同型なもののいくつかに分解されるが，その分解から次のような位数３の $V^\natural$ の自己同型 τ_S が定義できるのである。

$L(\frac{4}{5},0)\oplus L(\frac{4}{5},3), L(\frac{4}{5},\frac{2}{5})\oplus L(\frac{4}{5},\frac{7}{5})$ の上では恒等変換

$L(\frac{4}{5},\frac{2}{3})^+, L(\frac{4}{5},\frac{1}{15})^+$ の上では ω 倍

$L(\frac{4}{5},\frac{2}{3})^-, L(\frac{4}{5},\frac{1}{15})^-$ の上では ω^2 倍

これが Monster の $3A$ 元を与えている。

次に τ_S の固定空間を考える。固定空間もまた VOA の構造を持つ。今度はそこに位数2の自己同型 σ_S が定義できるのである。

$L(\frac{4}{5},0), L(\frac{4}{5},\frac{7}{5})$ の上では恒等変換

$L(\frac{4}{5},3), L(\frac{4}{5},\frac{2}{5})$ の上では -1 倍

もちろん，これは Monster の元ではない。しかし，Monster の元 τ_S と対応していることは確かである。

そこで，1節で述べたような elementary abelian group E_W を考える，その $3A$ 元は，今述べた τ_S の形で与えられる，E_W の固定空間をとると，そこには σ_S たちが作用することになる。これらは，どのような群を生成するのだろうか。実は，このことに関する一般論はまだなく，答えはわからない。しかし，1節で述べたような E_W の構造を考えると，$\Omega^-(6,3).2$ という群が出てくるのが自然だと思うのである。

同様の話として2節の内容に関するものはすでにあって，それはほぼ完成された形になっている。

$V^\natural$ の subVOA として $T = L(\frac{1}{2},0)$ という構造のものが存在し，その規約加群は同型を除いて，

$$L(\frac{1}{2},0), L(\frac{1}{2},\frac{1}{2}), L(\frac{1}{2},\frac{1}{16})$$

の3種類のいずれかに同型である。$V^\natural$ を T-加群として分解すれば，そこから次のような位数2の自己同型 τ_T が定義できる。

$L(\frac{1}{2},0), L(\frac{1}{2},\frac{1}{2})$ の上では恒等変換

$L(\frac{1}{2},\frac{1}{16})$ の上では -1 倍

これが Monster の $2A$-元を与えてる。

τ_T の固定空間には，また新しい位数2の自己同型 σ_T が定義できる。

$L(\frac{1}{2},0)$ の上では恒等変換

$L(\frac{1}{2},\frac{1}{2})$ の上では -1 倍

そこで，2節のように E_W と，その固定空間を考える。ただし，E_W としては $2A$ 元を含むものをとる。従って，Γ_W として $\sqrt{2}\Gamma_{24}$ が現れるものは考えない。そうすると，そこには $2A$ 元に対応して σ_T たちが作用しているのであるが，それらの性質は宮本氏により決定されており，3-transposition group になるという一般論がある。実際，σ_T たちは対応する sublattice Γ_W の root に関する reflection group の2群による拡大を生成する。

さらに，いくつかの場合にはこの固定空間の VOA の構造も完全に記述できて，いわゆる binary code VOA として構成される。

このように，一方には Niemeier lattice や code VOA といった完成された形の数学が存在するので，その complex version, binary version がないだろうか，というのが本稿の主題なのである。簡単に言ってしまえば２と３の違いだけなのだが，実現するにはまだアイディアが足りないようである。

最後に文献をいくつかあげておく。

[1] J.H.Conway, N.J.A.Sloane, Sphere Packings, Lattices and Groups, Springer

Code, lattice については，この１冊をあげればほぼ十分だろう。近々第３版が出るようである。

[2] C. Dong, H. Li, G. Mason and S.P. Norton, Associative subalgebras of the Griess algebra and related topics, preprint.

Leech lattice に Niemeier lattice の $\sqrt{2}$ 倍が含まれることはこの論文に記述がある。

[3] M.Miyamoto, Griess algebras and conformal vectors in vertex operator algebras, *J. Algebra*, **179** (1996) 523-548.

[4] M.Miyamoto, Binary codes and vertex operator (super)algebras, *J. Algebra*, **181** (1996) 207-222.

[5] M.Miyamoto, 3-State Potts model and automorphism of vertex operator algebra of order 3, preprint.

[6] M.Miyamoto, A new construction of the moonshine vertex operator algebra over the real number field, preprint.

宮本氏の理論については代表的なものを４つ挙げた。

[7] M.Kitazume, M.Miyamoto, H.Yamada, Ternary codes and vertex operator algebras, preprint.

これは ternary case の一つの試みである。

準結晶入門

放送大学・埼玉学習センター　331-0851　大宮市錦町 682-2
堂寺知成（物理学）　dotera@u-air.ac.jp

正五角形による平面のタイル張りはできない。正二十面体による三次元空間充填はできない。したがって、それらの持つ５回対称性がマクロな物質には現れるはずがない、と長らく信じられてきた。しかし、1984 年シェヒトマンらによってアルミ系合金に発見された準結晶は、正二十面体対称性（５回対称性）を有し、さらにその構造が、1970 年代に重力理論で有名なペンローズの発見した非周期的タイリング（図１）との関連がシュタインハートらに指摘されるに及んで、物理学の分野で大きなセンセーションを巻き起こした。また、１方向は周期性をもつが、残りの２次元面に５回対称性がある２次元準結晶も発見されている。80 年代の後半には熱力学的安定準結晶が発見され、それ以来、多くの構造的に安定で欠陥の少ない準結晶が作られ現在に至っている。（参考文献１）

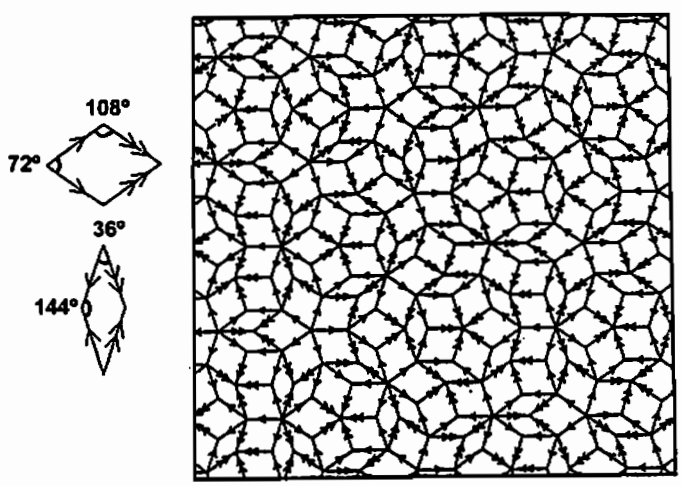


図１　２種類の菱形で作られるペンローズのタイル張り

８０年代の興奮の大きなうねりのあと９０年代のやや落ち着いた研究を総括してみると、「物質はたくさん発見されたが、満足しうる理論（と実験）がない」というのが準結晶物理学の現状である。従来の結晶を中心に据えた物理理論がフーリエ展開に大きく依存しているために使えない困難もある。準結晶の熱力学的安定性の起源に関する論争（エネルギー対エントロピー論争）の決着もついておらず、結晶のように構造が決定されるべきかどうか、ランダム系であるアモルファスのように本質的に原子配置の乱れているのかどうかすらわかっていない。物理学者にとっては必須の物と言っていいだろうが、物質構造解明の道具立としては「高次元結晶学」が成立し、それを利用しておおよその構造はわかってきたものの、構造決定問題は誰もが納得し得る状況には程遠い。従って、構造を仮定して計算しなければならない物理的性質の議論も隔靴掻痒の感が

ある。さらに実験が進歩するにつれ、準結晶の複雑さ、微妙さがますます明らかになり、それまでの結果が次々に更新され、信頼すべきデータがないといった理論家の嘆きも聞こえてくる。

そういった物理学としてはまだ夜明け前の感じがするのであるが、例えば超伝導のような応用はないわけで、発見より１０年以上を経て、アメリカなどでは物理学者が予算を得て研究する分野ではなくなっている。しかし、人は減っても解明すべき基本的（数学的な）問題は事欠かないとわけで、フランス・ドイツなどは元気がいい。

かつて、マーチン・ガードナーがサイエンティフィック・アメリカン誌にペンローズの非周期的タイル張りやコンウェイの研究を紹介したこともあり、書店においては数学のコーナーに準結晶の驚きを記述した書物が多い。予想外かもしれないが、数学者の方が普通の物理学者よりも準結晶について聞いたことがある、という面もないとは言えない。物理学が停滞しはじめた今、実験とは無関係に、準結晶の一番の特徴である準周期性の数学的基礎理論を構築が望まれる。一次元準周期系から始まって、ペンローズの発見した非周期的タイリングに代表される準周期タイル張り、それらの数学的性質の解明が残されているように思われる。

この報告書では、簡単に準周期性、一次元準結晶を紹介し、加えて筆者が導いた自己相似多項式について記述する。最後に準結晶特有の乱れであるフェイゾン乱れとその応用について、短い紹介を述べる。

準周期性

最初に準周期性の定義を少し思い出してみよう：アフィン（d 次元）空間$\mathbf{E}_c$上の（d 実変数の）関数が、高次元空間$\mathbf{R}^n$で定義されたｎ実変数の周期関数の（アフィン部分空間として埋め込まれた）$\mathbf{E}_c$への制限である時、その関数は「準周期的」である。もちろん埋め込まれた空間$\mathbf{E}_c$（カット）が周期関数の周期の格子に有理数の傾きを持つなら、つまり$\mathbf{E}_c$が格子からなる部分空間に平行なら、この関数の$\mathbf{E}_c$への制限もまた周期的である。しかし、カットの方向が無理数的なら、つまり、カットに平行なベクトル部分空間が原点以外の格子点を一つも含まないなら、この制限は周期関数ではない。たとえば、ｘとｙの２実変数関数ｆを考える：

$$f(x,y)=\cos x+\cos\sqrt{2}y \qquad (1)$$

この関数は（ｘ、ｙ）平面では周期的である。われわれはｙ＝ｘ上の「対角線」的制限をとる。この関数φは一変数ｘの$\phi(x)=\cos x+\cos\sqrt{2}x$なる関数で周期的ではない。というのもコサイン関数の二つの角変数が不整合だからで、このφは準周期関数である。

準結晶物理学の最も有用な道具は上記の定義に基づいている。つまり、高次

元結晶学の「射影法」による準周期タイルの構成法は、E_cに沿う$(n-d)$次元の窓に含まれるR^nの内の格子Λの点を集めることにある（図２）。これは単にさまざまなダイルを生み出す方法として用いられるばかりでなく、（物理的意義については疑義もあるのだが）窓の形を定めて、原子を配置する方法が、現在の原子構造決定の有力な方法となっている。また、あとで述べるフェイゾン乱れは窓の乱れ（ボケ）として考えることができる。

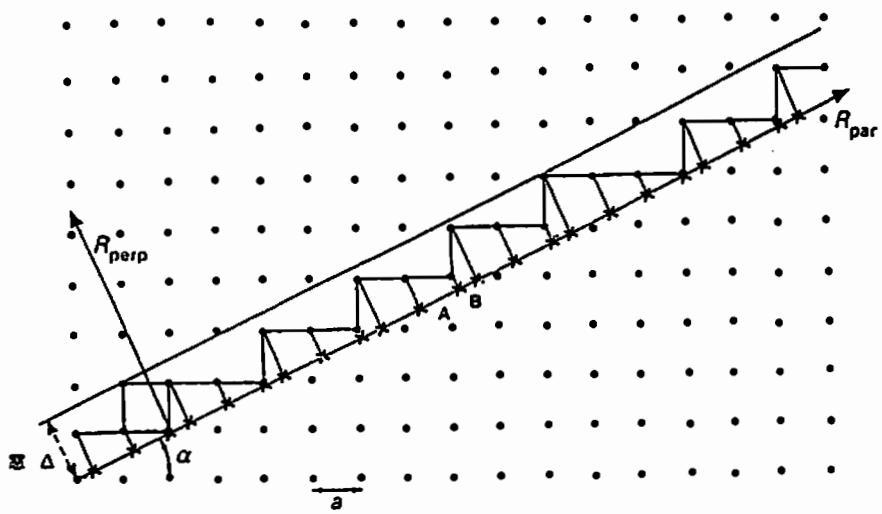


図２　射影法によって作られた一次元準結晶

最も典型的で自然界にあらわれる準結晶に一番つながりの深いフィボナッチ準結晶は、図２のように、正方格子に黄金比の逆数（ロシアではそれを黄金比という）の傾きを持つ許容窓をとればよいのであるが、射影法では計算機を用いないとフィボナッチ準結晶さえ作れないことが難点である。

一次元結晶列

有限の文字列、これを単位列とよぶことにするが、単位列の周期的繰り返しで表わされる文字列をここでは結晶とよぶ。物理学的には、なぜ、結晶ができるのか？というのは非自明なことであって、量子力学的に議論すべきことであるはずだし、物理学的にもいろいろと難しい議論もある。しかし、ひとつのおもちゃモデルとして、簡単な仕組みを述べてみよう。

結晶文字列の構成法は決定論的であり、列の中の周りの環境も含めたある文字の配置は、全く同じ配置が必ず、繰り返しの数と同じだけ存在する。このことはある原子の（局所的）配置がエネルギー的に好ましいものであった場合、それが繰り返して結晶配列ができるとしたならば全体としてもエネルギー的に好ましいという結果をもたらす。一方、ランダム列では種々の原子環境が存在

するが、エネルギー的にそのすべてが好ましいものである可能性がすくないから、不安定になるのである。

以上のことを考える、すべての準周期タイル（対称性、局所配置）が自然界に実現されるわけではない。物質の準結晶がなぜ２０面体対称性を持つかというと、準結晶に含まれる原子クラスターとして２０面体対称性を持つものが存在するからである。準結晶においてもなるべく少ない（局所的）配置で全体の非周期的タイルが構成されることが望ましい。つまり、物理的には、原子クラスターの配列の仕方がなるべく少ない組み合わせで構成される準結晶構造が選ばれている可能性が高い。

ここでは詳しく記述できないが、こういった局所的配置の要請からも性質のよい、２０面体対称性と深い関わりのある、基本的な一次元準結晶のフィボナッチ準結晶、二次元準結晶のペンローズタイルの研究には意味がある。

一次元準結晶（フィボナッチ準結晶）

フィボナッチ数f_nは

$$f_{n+2} = f_n + f_{n+1}、\ f_1 = 1、\ f_2 = 2$$

で定義される。これはウサギの問題として始まったことが伝えられている。すなわち、A(Adult)、B(Baby)が一世代経るごとに次のように置き換えられる。

$$\begin{cases} \mathbf{A} \rightarrow \mathbf{BA} \\ \mathbf{B} \rightarrow \mathbf{A} \end{cases}、$$

これは自己相似性のあからさまな構成法であるが、同等なものとして次の方法がある。文字列$\mathbf{S}_n$を考えよう。前の二つの文字列をつなげ、

$$\mathbf{S}_n = \mathbf{S}_{n-2}\mathbf{S}_{n-1}$$

で列を生成する。ここで、$\mathbf{S}_0 = \mathbf{B}$、$\mathbf{S}_1 = \mathbf{A}$として具体的に書けば、

$$\begin{aligned} \mathbf{S}_0 &= \mathbf{B} \\ \mathbf{S}_1 &= \mathbf{A} \\ \mathbf{S}_2 &= \mathbf{BA} \\ \mathbf{S}_3 &= \mathbf{ABA} \\ \mathbf{S}_4 &= \mathbf{BAABA} \\ \cdots &\quad \cdots \end{aligned}$$

となる。

文字A、Bの数の比は連続するフィボナッチ数の比であり、この（半）無限列の極限では、その比は良く知られた黄金比

$$\tau = \frac{1+\sqrt{5}}{2} = 1.618\cdots$$

に収束する。５角形の対角線の分割にこの比が現れることは良く知られている。

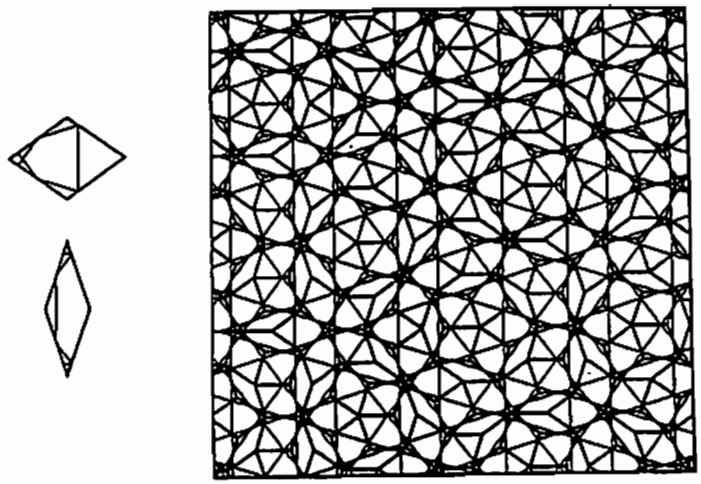


図3　ペンローズタイルにも5方向にフィボナッチ準結晶の配列が隠れている。

リー群上のフィボナッチ列

$M_n \in \mathrm{SL}(2)$に対して、

$$\mathbf{M}_n = \mathbf{M}_{n-2}\mathbf{M}_{n-1}$$

で定義される行列のフィボナッチ列のトレース

$$F_n = tr\mathbf{M}_n$$

には、

$$F_{n+2} = F_{n+1}F_n - F_{n-1}$$

が成り立つ。これを物理では、Kohmoto,Kadanoff&Tang のトレース公式（漸化式）とよばれ、一次元準結晶の電子論などの研究に役立つ方程式である。この漸化式には、

$$I = F_{n+2}{}^2 + F_{n+1}{}^2 + F_n{}^2 - F_{n+2}F_{n+1}F_n$$

なるnに関する不変量がある。漸化式を力学系を記述する方程式と見立て、不変量の作る面の上を動く軌道の周期点やカオス的ふるまいを調べるという見方もある。ここまでが良く知られている事実で、ここから（無意味な一般化など含めて）膨大な数理的研究が派生した。参考文献2を御覧いただきい。

物理学としては、固有値問題として、周期系の連続スペクトル、ランダム系の点スペクトルの狭間にある「特異連続スペクトル」としておおいなる興味を惹いた。実際、きれいな準結晶ほど抵抗値が高く（結晶と逆の振るまい）、しかも金属系でありながら、ランダム系（アモルファス）よりも抵抗が大きく、半導体的振る舞いをしめす。特異連続スペクトルが、そのような性質をひき起こす原因の一部である可能性は高い。

自己相似多項式

さて、物理を離れて数理的興味あるいフィボナッチに見せられたマニアとして、一般化ではなく、上のフィボナッチ系の漸化式の背後にある数理を次に考えよう。

先ず、非対角成分について、$trP=0$なる行列を用いると、

$$G_n = tr(\mathbf{PM}_n) = tr(\mathbf{PM}_{n-2}\mathbf{M}_{n-1}),\quad H_n = tr(\mathbf{M}_{n-2}\mathbf{PM}_{n-1})$$

について、先のトレース公式も含めて書けば、

$$F_{n+2} = F_{n+1}F_n - F_{n-1}$$

$$G_{n+2} = F_{n+1}G_n + G_{n-1}$$

$$H_{n+2} = G_{n+1}F_n - G_{n-1}$$

となっている。不変量は

$$I = {F_{n+2}}^2 + {F_{n+1}}^2 + F_n^2 - F_{n+2}F_{n+1}F_n$$

$$\begin{aligned} J &= (-1)^n\left(-F_{n+2}G_{n+2} + F_{n+1}G_{n+1} - F_nG_n + F_{n+2}F_{n+1}G_n\right) \\ &= (-1)^n\left(F_{n+2}H_{n+2} + F_{n+1}G_{n+1} - F_nG_n - F_{n+2}G_{n+1}F_n\right) \end{aligned}$$

となる。

ここで、物理の筋の良い電子問題からでてきた初期値の行列として、

$$\mathbf{M}_1 = \begin{pmatrix} x & -1 \\ 1 & 0 \end{pmatrix},\quad \mathbf{M}_2 = \begin{pmatrix} x & -1/r \\ 1 & 0 \end{pmatrix}\begin{pmatrix} rx & -r \\ 1 & 0 \end{pmatrix},\quad r \neq 1$$

を採用する。rは準結晶性の強さの程度を表すパラメータで、$r=1$は結晶に対応する。xは物理的にはエネルギースペクトルに対応するのであるが、ここでは実変数と思っていただいてよい。また物理的意味が不明なのであるが、

$$\mathbf{P} = \begin{pmatrix} -2r^2x^2+1 & 2x\left(r^2x^2-1\right) \\ -2r^2x & 2r^2x^2-1 \end{pmatrix}$$

を採用すると、次の種関数（seed functions）が得られる。

$$\begin{array}{lll} F_1(x) = x & F_2(x) = rx^2 - r - 1/r & F_3(x) = rx^3 - (2r+1/r)x \\ G_1(x) = \left(2r^2-1\right)x & G_2(x) = rx^2 + r - 1/r & G_3(x) = \left(2r^3-r\right)x^3 + \left(-2r^3+1/r\right)x \\ H_1(x) = x & H_2(x) = \left(2r^3-r\right)x^2 + 1/r - r & H_3(x) = rx^3 - x/r \end{array}$$

$$I = (r+1/r)^2,\quad J = (r+1/r)(r-1/r)$$

これらと漸化式で得られる多項式$F_n(x)$を第1種の自己相似多項式、$G_n(x)$、$H_n(x)$を第2種の「自己相似多項式」と呼ぶことにする。

これらの自己相似多項式の性質として次のもの（1）～（3）がある。

（1）$r=1$のとき、$F_n(x)$はフィボナッチ数番目の第1種のChebyshevの多項式に一致し、$G_n(x)$、$H_n(x)$はフィボナッチ数番目の第2種のChebyshevの多項式に一致する。この意味で、自己相似多項式はChebyshevの多項式の準結晶的拡張になっている。（結晶の世界では一致していたG_nとH_nも準結晶では一致しない。）

従って、トレース公式はなんのことはない三角関数の加法定理

$$2\cos(\alpha+\beta)=2\cos\alpha\cdot 2\cos\beta-2\cos(\alpha-\beta)$$
$$2\sin(\alpha+\beta)=2\cos\alpha\cdot 2\sin\beta+2\sin(\alpha-\beta)$$
$$2\sin(\alpha+\beta)=2\sin\alpha\cdot 2\cos\beta-2\sin(\alpha-\beta)$$

に対応したものであることがわかる。

（2）$r\ll 1$のとき、これは準結晶性が強い場合であるが、$F_n(x)$、$G_n(x)$、$H_n(x)$は次のような意味で自己相似性をもつ。

（a）3サイクル：$|x|<|r|\ll 1$の条件のもとで

$$F_4(x)\cong F_1(x/r^2)\quad F_5(x)\cong -F_2(x/r^2)\quad F_6(x)\cong -F_3(x/r^2)$$
$$G_4(x)\cong -G_1(x/r^2)\quad G_5(x)\cong G_2(x/r^2)\quad G_6(x)\cong G_3(x/r^2)$$
$$H_4(x)\cong -H_1(x/r^2)\quad H_5(x)\cong H_2(x/r^2)\quad H_6(x)\cong H_3(x/r^2)$$

となる。

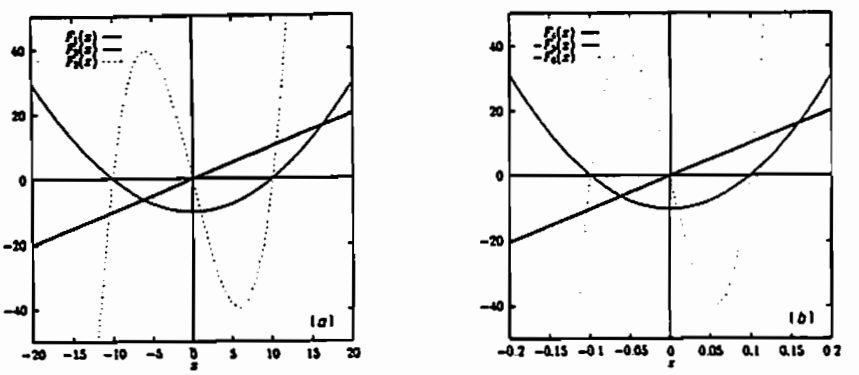


図4　自己相似多項式の自己相似性（3サイクル）（$r=1/10$）：（左）種関数（$n=1,2,3$）と多項式（$n=4,5,6$）の中心部分の100倍の拡大図。

蛇足にはなるが、$|x|<|r|\ll 1$のもとでは種関数は次のように近似できて、

$$\tilde{F}_1(x)=x \quad \tilde{F}_2(x)=-r-1/r \quad \tilde{F}_3(x)=-x/r$$
$$\tilde{G}_1(x)=-x \quad \tilde{G}_2(x)=r-1/r \quad \tilde{G}_3(x)=x/r$$
$$\tilde{H}_1(x)=x \quad \tilde{H}_2(x)=1/r-r \quad \tilde{H}_3(x)=-x/r$$

となる。ここから

$$\tilde{F}_4(x)=F_1(x/r^2) \quad \tilde{F}_5(x)=-F_2(x/r^2) \quad \tilde{F}_6(x)=-F_3(x/r^2)$$
$$\tilde{G}_4(x)=-G_1(x/r^2) \quad \tilde{G}_5(x)=G_2(x/r^2) \quad \tilde{G}_6(x)=G_3(x/r^2)$$
$$\tilde{H}_4(x)=-H_1(x/r^2) \quad \tilde{H}_5(x)=H_2(x/r^2) \quad \tilde{H}_6(x)=H_3(x/r^2)$$

が等号の付いた式が計算できる。

（b）2サイクル：$|x|<|r|\ll 1$の条件のもとで

$$F_3(x\pm R)\cong F_1(2x/r) \quad F_4(x\pm R)\cong \pm F_2(2x/r) \quad F_5(x\pm R)\cong \pm F_3(2x/r)$$
$$G_3(x\pm R)\cong G_1(2x/r) \quad G_4(x\pm R)\cong \pm G_2(2x/r) \quad G_5(x\pm R)\cong \pm G_3(2x/r)$$
$$H_3(x\pm R)\cong H_1(2x/r) \quad H_4(x\pm R)\cong \pm H_2(2x/r) \quad H_5(x\pm R)\cong \pm H_3(2x/r)$$

となる。ここで$R=r+1/r$である。

ここでも$|x|<|r|\ll 1$のもとでは種関数は次のように近似できて、

$$\tilde{F}_1(x)=\pm(r+1/r) \quad \tilde{F}_2(x)=\pm 2x \quad \tilde{F}_3(x)=2x/r$$
$$\tilde{G}_1(x)=\pm(r-1/r) \quad \tilde{G}_2(x)=\pm 2x \quad \tilde{G}_3(x)=(4r-2/r)x$$
$$\tilde{H}_1(x)=\pm(r+1/r) \quad \tilde{H}_2(x)=\mp 2x \quad \tilde{H}_3(x)=2x/r$$

となる。ここから

$$\tilde{F}_3(x)=F_1(2x/r) \quad \tilde{F}_4(x)=\pm F_2(2x/r) \quad \tilde{F}_5(x)=\pm F_3(2x/r)$$
$$\tilde{G}_3(x)=G_1(2x/r) \quad \tilde{G}_4(x)=\pm G_2(2x/r) \quad \tilde{G}_5(x)=\pm G_3(2x/r)$$
$$\tilde{H}_3(x)=H_1(2x/r) \quad \tilde{H}_4(x)=\pm H_2(2x/r) \quad \tilde{H}_5(x)=\pm H_3(2x/r)$$

が計算できる。

準周期性が強い場合には、つねに種関数がたち現われるという意味で、種関数は漸化式の固定点関数とも言い得るだろう。これら3サイクルと2サイクルの二つのスケーリング定数を持つバイ・フラクタルな自己相似性の構造を模式化すると、フィボナッチの木と呼ばれる構造となり、それはまさしくフィボナッチ準結晶の自己相似性を反映したものであることもわかる。

（3）第1種のChebyshevの多項式はその零点に関して直交性を持つことが知られている。第1種の自己相似多項式$F_n(x)$はそのゼロ点に関して直交性を持たないものの、その内積の値はフィボナッチ数と類似する数列およびパラメーターrで書くことが出来ることが数値的に示されている。証明はない。

以上は鈴木寿一氏と筆者の結果である。詳しくは文献5にある。

フェイゾン乱れ

フィボナッチ準結晶でのフェイゾン乱れとは、正しい列において、文字列の順序を入れ替えることである。すなわち一番小さいフェイゾン乱れは

$$A \leftrightarrow B$$

である。2次元以上でもタイルの並べ替えという形で存在する。実際の物質では熱的乱れが存在し、多かれ少なかれフェイゾン乱れがある。

理論的困難としては、第一にフェイゾン乱れが結晶における転位のように基本群で特徴付けられないことがある。その他、タイル張り、並べ換えに関連したフェイゾン乱れの生み出す面白い性質は文献6、7にある。

フェイゾンの応用：準結晶⇒結晶変換

物質には変態するという性質があり、熱的相変態、力を加えたときの塑性変形などがある。それらに関連して筆者が最近興味をもっていることを最後に紹介しよう。

まず、フィボナッチ準結晶の半無限列を考える。先に紹介したものとは左右が逆になっていることに注意する。

ABAABABAABAABABAABABAABAABABAABAAB…

次に東大物性研河野研究室で発案された変換を考える。それは、フィボナッチ準結晶列の中に下の左の文字列がある場合、すべて右の文字列に置き換える。

$$AAB \rightarrow ABA$$

すると次の列ができる。

AB|ABAABABAABAABABAABABAABAABABAABAAB…

これはABが左に出て、2文字フィボナッチ準結晶が右に移動する。これを繰り返せば、

AB|AB|AB|AB|AB|AB|ABAABABAABAABABAABABAABAABABAABAAB…

のように、左にAB結晶がフィボナッチ準結晶から吐き出されてくる。一般化は容易で、

$$BA \rightarrow AB$$

とすれば、A結晶が、

$$ABABA \rightarrow ABAAB$$

とすれば、ABA結晶が、

$$ABAABAAB \rightarrow ABAABABA$$

とすれば、ABAAB結晶が生じる。

これに関連した2次元のシミュレーションは文献8にある。

参考文献

1）実験の写真を是非御覧下さい。蔡安邦「準結晶はどこまで解明されたか」日経サイエンス 1996 年 7 月号。

2）数理物理(後半は一次元準結晶）の興味からは次の本がよい。「Beyond Quasicrystals」、F.Axel and D.Gratias eds.、Springer & Les Editions de Physique Les Ulis 1995。

3）物理学として準結晶理論概観という意味では次の本がよい。「Lectures on Quasicrystals」、F.Hippert and D.Gratias eds.、Les Editions de Physique Les Ulis 1994。

4）簡単な数学（タイリングの紹介）の教科書としては次のものがある。「Quasicrystals and Geometry」、M.Senechal、Cambridge 1995。

5）自己相似多項式については、次の二つを見て下さい。T.-k. Suzuki and T. Dotera、J.Phys.A: Math. Gen.26、6101 (1993)； T. Dotera、Phys.Rev. B38、11534 (1988)。

6）T. Dotera and P. J. Steinhardt、「Ising-Like Transition and Phason Unlocking in Icosahedral Quasicrystals」、Physical Review Letters, Vol.72 (1994) p. 1670。

7）T. Dotera, Hyeong-Chai Jeong, and Paul J. Steinhardt、「Properties of Decapod Defects」、*Methods of Structural Analysis of Modulated Structures and Quasicrystals*, pp. 660-666, J. M. Perez-Mato, F. J. Zuniga, and G. Madariaga ed. World Scientific(1991)。

8）T. Dotera、「Can Quasicrystals Flow?」、*Quasicrystals*, T.Fujiwara and S.Takeuchi, eds. World Scientific (1997)。

Pisot数とフラクタルタイリング*

秋山 茂樹

平成10年 11月 5日

1 一様分布論と Pisot 数

Pisot 数を定義する前に一様分布論を復習しよう。[1] 実数列 (u_n) $n = 1, 2, \ldots$ を考える。$0 \leq a < b \leq 1$ なる a, b に対し $\chi_{[a,b]}$ を閉区間 $[a, b]$ の characterictic function すなわち

$$\chi(x) = \begin{cases} 1, & x \in [a, b] \\ 0, & x \notin [a, b] \end{cases}$$

と定義する。このとき

定義 (u_n) が一様分布する（以下 $u_n : u.d.$ mod 1 と書く）とは

$$\lim_{N \to \infty} \sum_{n=1}^{N} \chi_{[a,b]}(\{u_n\}) = \int_0^1 \chi_{[a,b]}(x)dx = b - a$$

が任意の $0 \leq a < b \leq 1$ に対して成立することをいう。ここで $\{x\}$ は x の小数部分である。

明らかにこれは (u_n) の小数部分が一様に $[0, 1)$ に分布している事を表している。いかなる列が一様分布するのかは興味深い数論の問題である。最初の基本的結果を導いたのは H.Weyl であった。

定理(Weyl) $(u_n) : u.d.$ mod 1 であることは以下と同値である。全ての $[0, 1]$ で Riemann 可積分な関数 f に対して

$$\lim_{N \to \infty} \sum_{n=1}^{N} f(\{u_n\}) = \int_0^1 f(x)dx$$

これでは定義よりも調べる関数を増やしたようであるが、実際には特殊な関数だけ調べればよい。すなわち

定理(Weyl) $(u_n) : u.d.$ mod 1 は以下と同値である。全ての $h = 1, 2, 3, \ldots$ に対して

$$\lim_{N \to \infty} \sum_{n=1}^{N} \exp(2\pi\sqrt{-1}hu_n) = 0$$

---

*このノートは、金沢大学で行われたシンポジウム「代数的組合せ論」6月22日-25日 (1998) で行った Pisot 数全般に関するかなり私的な survey をまとめたものである。

[1] この節及び次節の結果に関しては [11], [7] を参照。また一様分布論に関するより新しい結果は [9] を見よ。

この定理は Weyl の規準と呼ばれている。一様分布論の重要な部分はこの規準を多くの関数に適用するため様々の巧妙な工夫を行うことに注がれる。ここではこれについては詳述しないが、多項式オーダーの増加関数に関しては一様分布がある程度多くのクラスで証明されており、指数オーダーの増加関数では結果は知られていない。一方、測度論的結果は指数オーダーでも存在する。

定理 (Koksma) t を閉区間 $[a,b]$ に値をとるパラメータとする。$f_n(t)\quad n=1,2,\ldots$ は実数値関数列で各 $f_n(t)$ は t に関して微分可能とする。さらに全ての $m,n\ (m\neq n)$ について $f'_m(t)-f'_n(t)$ は t の単調関数であるとし、ある $K>0$ が存在して全ての $m,n\ (m\neq n)$ および全ての $t\in[a,b]$ について

$$|f'_m(t)-f'_n(t)|>K$$

が成立するならば測度零の例外を除いて全ての $t\in[a,b]$ について数列 $(f_n(t))\quad n=1,2,\ldots$ は一様分布する。

この定理から次はすぐに従う。

系1. $\alpha>1$ を固定するとき $(\lambda\alpha^n)\quad n=1,2,\ldots$ はほとんど全ての実数 λ に関して一様分布する。

系2. $\lambda\neq 0$ を固定する。このとき $(\lambda\alpha^n)\quad n=1,2,\ldots$ はほとんど全ての$\alpha>1$ に対して一様分布する。

ここで、「ほとんど全て」というのは、測度零の例外を除いてという意味で用いている。特に系2. からほとんど全ての$\alpha>1$ に対して $(\alpha^n)\quad n=1,2,\ldots$ は一様分布するが、(やや驚くべきことに) 一つとして具体的に (α^n) が一様分布する α は知られていないのである。[2]

未解決問題 $((\frac{3}{2})^n)$ や (e^n) は一様分布するか？

しかしながら (α^n) が一様分布しない例は無限に存在する。たとえば α を 2 以上の整数とすれば小数部分はないので明らかに一様分布ではない。だがもっと非自明な例もある。

例 ω を黄金比 $\frac{1+\sqrt{5}}{2}$ とする。このとき $\|\omega^n\|\to 0$ が成り立つ。ここで $\|x\|$ は x と整数との距離である。

この現象は ω が Pisot 数と呼ばれる Koksma の定理の例外集合に属する事から生じる。

定義 実数 $\beta>1$ が Pisot(-Vijayaraghavan) 数であるとは、代数的整数であって自分自身と異なる共役の絶対値が 1 より小のときいう。また実数 $\beta>1$ が Salem 数であるとは、代数的整数であって自分自身と異なる共役の絶対値が 1 以下であって少なくとも一つの共役の絶対値が1 であるものをいう。

例 $\omega=\frac{1+\sqrt{5}}{2}=1.618033988\cdots$ の共役は$\omega'=\frac{1-\sqrt{5}}{2}$ であって $|\omega'|<1$。したがってω は Pisot 数である。また$x^4-x^3-x^2-x+1$ の 1 より大な実数根

$$\frac{1+\sqrt{13}}{4}+\frac{1}{2}\sqrt{\frac{\sqrt{13}-1}{2}}=1.7220838\cdots$$

[2]講演でこのように述べたのですが、この認識はいささか古かったようです。M.Levin が (α^n) がこのような α を具体的に構成していました。さらに彼の構成したものは一様分布より強い完全一様分布という性質を満たし、その Discrepancy も最善に近い上からの評価を持ちます。[9] の 118p-138p をご覧下さい。ただし、彼の構成法は具体的とはいえ α の値を順に精密に決定していくプロセスの存在証明であって、その数の数論的性質は分かりません。

は Salem 数である。

このとき次が証明できる。

命題 α が Pisot 数ならば $\lim_{n\to\infty}||\alpha^n|| = 0$ がなりたつ。また α が Salem 数ならば α^n の小数部分 $\{\alpha^n\}$ は $[0,1)$ に彫密に分布するが、(α^n) は一様分布しない。

この立場からは重要な未解決予想は

予想 $\lim_{n\to\infty}||\alpha^n|| = 0$ ならば α は Pisot 数である。

というものである。この予想に対するアタックの到達点を紹介しよう。

定理 (Cantor, Decomp-Guilloax, Grandet-Hugot [7]) 実数 $\alpha > 1$ に対して、ある $\lambda \geq 1$ が存在して全ての $n = 0, 1, 2, \ldots$ について

$$||\lambda\alpha^n|| \leq \frac{1}{2e\alpha(\alpha+1)(1+\log\lambda)}$$

が成立することと α が Pisot 数または Salem 数であることは同値である。

この定理からは次が従う。

系 $||\alpha^n|| = o(\frac{1}{n})$ ならば α は Pisot 数である。

この系は $||\alpha^n||$ が 0 に近づくだけでなくそのスピードが充分速ければPisot数になってしまうことを主張している。このスピードを $o(\frac{1}{\sqrt{n}})$ に緩めても同じ主張が成立する事が知られている。

2 Pisot 数の分布について

Pisot 数に関して一般的に知られている事を幾つか紹介しよう。まず簡単な事実として

命題 実代数体は少なくとも一つの Pisot 単数を含む。

ここで Pisot 単数とは Pisot 数でそれを含む代数体において単数であることをいう。言い替えれば Pisot 単数とは Pisot 数でその最小多項式の定数項が ± 1 のものである。この Proposition の証明には Dirichlet の単数定理の標準的な証明を思い出せばよい。

さて Pisot 数の一般的な分布状況に関しては次の真に驚くべき結果が知られている。S を Pisot 数の全体のなす集合としよう。当然$S \subset [1,\infty)$ であるがさらに

定理 (Salem) S は $[1,\infty)$ で closed である。

この定理以前には S が $[1,\infty)$ で彫密であるのではないかと多くの数学者は漠然と思っていた。実際には S はこの定理により nowhere dense になってしまう。なぜならある点 x の近傍 U で彫密なら定理により $U \subset S$ となるがこの U には当然、整数でない有理数や代数的でない点が含まれてしまうので矛盾するからである。もう一つのやはり Salem によるなかなか納得しがたい定理がある。

定理(Salem)　任意の Pisot 数は Salem 数の集合の集積点である。

この逆に Salem 数が Pisot 数の集合 S の集積点という主張ならば、さもありなんという気がするのだが、実際にはこちらは正しくない。

さて S が $[1,\infty)$ で閉集合である以上最小の Pisot 数があるわけであるがこれは次で与えられる。

定理　最小の Pisot 数は x^3-x-1 の正根 $\theta=1.3247179572\ldots$ である。

この定理の最初の証明は C.L.Siegel によると人に聞いたが私には確認できなかった。いずれにせよ、かなり以前の結果であるが決して自明ではない。D.Boyd は任意の区間 $[a,b]$ を与えたときその中にある Pisot 数を決定するアルゴリズムを与えた。以下に小さい Pisot 数とその最小多項式の表を与える。近似値は ... 以下を切り捨ててある。

$1.324717957\ldots$	x^3-x-1
$1.380277569\ldots$	x^4-x^3-1
$1.443268791\ldots$	$x^5-x^4-x^3+x^2-1$
$1.465571231\ldots$	x^3-x^2-1
$1.501594803\ldots$	$x^6-x^5-x^4+x^2-1$
$1.534157744\ldots$	$x^5-x^3-x^2-x-1$
$1.545215649\ldots$	$x^7-x^6-x^5+x^2-1$
$1.561752067\ldots$	$x^6-2x^5+x^4-x^2+x-1$

さらに S の最小の集積点は黄金比 ω であることが知られている。

3　Pisot 数による数系

Pisot 数の様々な応用に関しては [7] に詳しい。以下に扱うのは、この本にはまだ載っていない未解決な問題の多い分野である。

まず任意の $\beta>1$ を固定する。すると任意の正数 x は $[0,\beta)$ の間の整数 a_i を用いて

$$x=\sum_{i=N_0}^{\infty}a_{-i}\beta^{-i}=a_{-N_0}\beta^{-N_0}+a_{-N_0-1}\beta^{-N_0-1}+\ldots$$

と展開される。ここではこの展開が全ての整数 $N\geq N_0$ に対して次を満たすものとする。

$$|x-\sum_{N_0}^{N}a_{-i}\beta^{-i}|<\beta^{-N}$$

このような展開を x の底 β による強欲展開 (greedy expansion) とよぶ。

例　$x=10,\beta=\sqrt{7}$ としよう。すると使える digit は $\{0,1,2\}$ であって

$$\begin{aligned} 10 &= 7+\sqrt{7}+\frac{2}{7}+\frac{1}{7\sqrt{7}}+\frac{1}{49\sqrt{7}}+\dots \\ &= \beta^2+\beta+2\beta^{-2}+\beta^{-3}+\beta^{-5}+\dots \\ &= 110.02101\dots \end{aligned}$$

となる。最後の表示は10進法などの表記に習って digit だけ並べたものでこのような表記を以下でも自由に用いる。なお、この展開は循環しないことが証明できる。([1])

さて $\beta>1$ を整数でない任意の実数としよう。$1-[\beta]/\beta$ を greedy に展開すると

$$\begin{aligned} 1-[\beta]/\beta &= b_{-2}\beta^{-2}+b_{-3}\beta^{-3}+\dots \quad (1) \\ &= \sum_{i=2}^{\infty} b_{-i}\beta^{-i} \quad (2) \end{aligned}$$

となるがここで $b_{-1}=[\beta]$ とおいて次のように定義する。

定義 $1=\sum_{-1}^{\infty} b_{-i}\beta^{-i}=.b_{-1}b_{-2}b_{-3}\dots$ を 1 の展開とよび $d(1,\beta)=.b_{-1}b_{-2}\dots$ と書く。

1 の展開は greedy expansion を実トーラス $\mathbf{R}/\mathbf{Z}\simeq[0,1)$ に働く力学系としてとらえるとき大事な役割を果たす事が知られている。([12]) 以下、1 の展開をその対応するワード $b_{-1}b_{-2}b_{-3}\dots$ と同一視する。

例 $\omega=(1+\sqrt{5})/2$ のとき $d(1,\omega)=.11$、最小 Pisot 数 θ の場合 $d(1,\theta)=.10001$ となる。

$[0,\beta)\cap\mathbf{Z}$ を用いたワードはどの出発点からみても $d(1,\beta)$ と比べ辞書式順序で小さいならばadmissibleという。greedy expansion によってできるワードはもはや繰り上がりがないので admissible となる。この逆も例外的な展開を除けば正しい。([12] をみよ。)

定義 $d(1,\beta)$ が有限のとき β のことを simple beta number という。また $d(1,\beta)$ が循環する展開（当然、有限の場合も含む）をもつならば β のことを cyclic beta number という。

このとき次が知られている。

定理(Parry) $[0,\infty)$ において simple beta number は彫密である。

定理(Parry) cyclic beta number の自分自身をのぞく共役の絶対値は 2 未満である。

前に述べた Salem の定理と比較すれば cyclic beta number は Pisot 数より随分多いことが分かる。この 2 という数字は黄金比 ω にまで改良できる。さて有理数の greedy 展開については次が知られている。

定理(A.Bertrand [8], K.Schmidt [14]) β を Pisot 数とするとき、実数 $x>0$ が循環することと x が $\mathbf{Q}(\beta)_{>0}$ に属することは同値である。

定理(K.Schmidt [14]) $\beta>1$ を任意の実数とする。全ての $x\in[0,1]\cap\mathbf{Q}$ が β を底とした greedy expansion で循環するならばβ は Pisot 数 または Salem 数である。

Salem 数の場合に全ての有理数が循環するか否かは重要な未解決問題である。いずれにせよ Pisot 数を底とする greedy 展開は興味深い研究対象である。以下 Pisot 数で任意の正数を展開する方法を Pisot 数系と呼ぶ。Pisot 数系の greedy 展開を調べていくうえで基本的な事の一つに、そもそも正整数の展開が有限なのかという問題がある。

定義 $\beta > 1$ を任意の実数とし、$\mathrm{Fin}(\beta)$ を全ての有限 greedy 展開のなす集合とする。

命題 (Frougny & Solomyak [10]) $\mathbf{Z}_{\geq 0} \subset \mathrm{Fin}(\beta)$ ならば β は Pisot 数または Salem 数である。

実はこの主張は次のように改善できる。

命題 (A [4]) $\mathbf{Z}_{\geq 0} \subset \mathrm{Fin}(\beta)$ ならば β は Pisot 数である。

この定理はなぜ Pisot 数系を特別視すべきなのかの理由を説明しているとも考えられる。次の条件を考える。

$$\text{(F)} \qquad \mathrm{Fin}(\beta) = \mathbf{Z}[\beta^{-1}]_{\geq 0}$$

この条件は 10 進法の $\beta = 10$ では自明である。一般にこの条件の成立を期待したいところであるが Pisot 数でもこの条件を満たさないものも多く存在する。(F) を満たす Pisot 数の代数的な特徴付けは満足のいく形にはできておらず重要課題の一つとなっている。以下 β は代数的とし $\mathrm{Irr}(\beta)$ を β の最小多項式 (係数は $\mathbf{Z}$) とする。このとき

定理 (Frougny & Solomyak [10]) $\mathrm{Irr}(\beta) = x^m - a_{m-1}x^{m-1} - a_{m-2}x^{m-2} - \ldots - a_0$ が $a_{i+1} \geq a_i \quad i = 0, 1, \ldots, m-2$ と $a_0 > 0$ を満たすならば、β は Pisot 数であって (F) を満たす。

という美しい定理がある。しかし、この条件は必要十分条件ではない。一般の Pisot 数の場合には次の方法で判定できる。

定理 (A, [3]) β が (F) を満たすことと次の有限集合の全ての元が有限展開されることは同値。

$$\left\{ x \in \mathbf{Z}[\beta] \;\middle|\; 0 < x = x^{(1)} < 1, |x^{(j)}| \leq \frac{[\beta]}{1 - |\beta^{(j)}|} \quad j = 2, 3, \ldots, m = \deg(\beta) \right\}$$

ここで $x^{(j)} \quad (j = 1, 2, \ldots, m)$ は $x \in \mathbf{Q}(\beta)$ の共役である。この定理は固定した Pisot 数が (F) を満たすかどうかの判定条件を与えるが、代数的な特徴付けでないので $\mathrm{Irr}(\beta)$ の形をみただけでは (F) を満たすかどうかは分からない。しかし私は最近この定理を用いて 3 次の Pisot 単数で (F) を満たすものを決定することができた。

定理 (A, [4]) β を 3 次の Pisot 単数とする。β が (F) を満たすための必要かつ充分な条件は最小多項式が以下の形をしているときである。

$$\mathrm{Irr}(\beta) = x^3 - ax^2 - bx - 1$$

かつ $-1 \leq b \leq a + 1$。

この節の最後に [1] の主定理を述べる。

定理(A, [1]) β が Pisot 単数で (F) を満たすとしよう。このときある正数 c が存在して $\forall x \in \mathbf{Q} \cap [0,c]$ の greedy expansion は純循環する。

この定理は、証明したときには気づいていなかったのだが以下に述べる Pisot 数の生成するタイル張りとも深く関係している。

4 Pisot 数によるタイル張り

以下の議論は次数 n の Pisot 数に対して可能であるがここでは説明を簡単にするため 3 次の Pisot 数で総実でないものとする。(一般論については [3] を参照。)

β を 3 次の総実でない Pisot 数で (F) を満たすものとする。一つの β の複素な共役を $\beta' \notin \mathbf{R}$ を固定する。Φ を β を β' に送る共役写像とする。さて β は (F) を満たすのであるから、$\mathrm{Fin}(\beta)$ の元をその小数部分に関して分類することで次の disjoint な分割を得る。

$$\mathrm{Fin}(\beta) = \bigsqcup S_\omega \tag{3}$$

ここで ω は S_ω の元の小数部分を表すワードで、たとえば.1 や .001 などである。但し ω が空語 λ の場合には S_λ は小数部分のない $\mathrm{Fin}(\beta)$ の元の集まりとする。この (3) の右辺の S_ω は、少し考えると平行移動による同値類は有限である事がわかる。さらに $\mathbf{R}_{\geq 0}$ の中で左辺は影密であるので closure をとると一次元タイル張り

$$\mathbf{R}_{\geq 0} = \bigsqcup \overline{S_\omega}$$

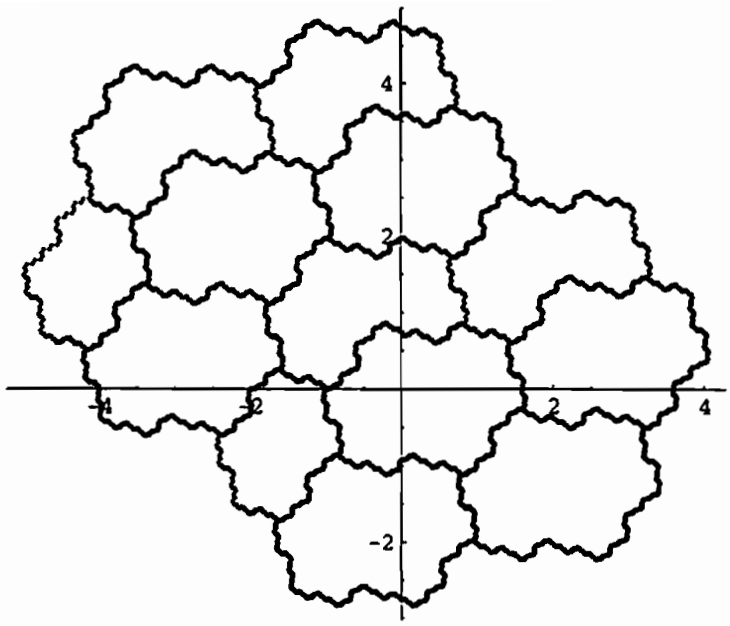
を得る。しかし各 S_ω は無論、有界でないので実態はよく分からない。そこで (3) の両辺に写像 Φ を施し、$\mathbf{C}$ で閉包をとると

$$\mathbf{C} = \bigsqcup \overline{\Phi(S_\omega)} \tag{4}$$

が得られる (証明は [2] と [3])。Pisot 数であるから $|\beta'| < 1$ ゆえ各 $\Phi(S_\omega)$ が有界なことに注意する。また Φ は体の同型写像なので (3) と同様、各 $\overline{\Phi(S_\omega)}$ は平行移動を除いて有限種類のコンパクトな集合からなる。さらに β が単数ならば次がわかる。

定理(A, [2]、一般には [3]) β を 3 次の総実でない Pisot 単数で (F) を満たすものとする。このとき原点は $\overline{\Phi(S_\lambda)}$ の内点である。

この事は大変基本的な事項でこれ用いると、各タイルの内点集合は影密であることや、各タイルの境界の 2 次元 Lebesgue 測度が零である事が証明される。すなわち有限種類のコンパクト集合の平行移動により複素平面がタイル張りされタイルの重なりは測度零なのである。現在筆者はこのようにして得られるフラクタルタイル張りに興味をもって研究中である。このタイル張りの絵の例を一つだけ描いておく。これは $\mathrm{Irr}(\beta) = x^3 - x^2 - x - 1$ の場合で G.Rauzy [13] により発見されたものであり現在 Rauzy fractal と呼ばれている。上に述べた基本的性質は図を見れば容易に納得できるだろう。上記のような formulation は [15] による。



これらのフラクタルに関しては何がわかり、何が問題なのかは論文 [2], [3] や数理研講究録[5], 早稲田大での研究集会報告 [6] でも書いたので重複を避ける。興味のある方はそちらを参照されたい。

参考文献

[1] S.Akiyama, Pisot numbers and greedy algorithm, Number Theory, Diophantine, Computational and Algebraic Aspects, Edited by K. Györy, A. Pethö and V.T.Sós, 9–21, de Gruyter 1998.

[2] S.Akiyama and T.Sadahiro, A self-similar tiling generated by the minimal Pisot number, to appear in Proceedings volume of 13th Czech and Slovak Conference on Number Theory, Acta Mathematica et Informatica Universitatis Ostraviensis.

[3] S.Akiyama, Self affine tiling and Pisot numeration system, to appear in 'Number Theory and its Applications', ed. by K. Gyory and S. Kanemitsu, Kluwer

[4] S.Akiyama, Cubic Pisot units with finite beta expansions, preprint.

[5] S.Akiyama, Pisot numeration system and self affine tiling (In Japanese), Surikaisekikenkyusho Kokyuroku No. 1060 (1998), 34–40.

[6] S.Akiyama, Pisot numeration system and Tamura's infinite product (In Japanese), Proceedings of the conference on number theory held at Waseda Univ. (1997) 78-86

[7] M.J.Bertin, A. Decomp-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse and J.P. Schreiber, Pisot and Salem numbers, Birkhäuser Verlag, Basel-Boston-Berlin 1992

[8] A.Bertrand, Dévelopment en base de Pisot et répartition modulo 1, C.R.Acad.Sc., Paris 385 (1977) 419–421

[9] M.Drmota and R.Tichy, Sequences, Discrepancies and Applications, Lecture Notes in Mathematics 1651, Springer

[10] C.Frougny and B.Solomyak, Finite beta-expansions, Ergod. Th. and Dynam. Sys. 12 (1992) 713–723

[11] L. Kuipers and H. Niederreiter, Uniform distribution of sequences. , Pure and Applied Math., John Wiley & Sons, (1974)

[12] W.Parry, On the β-expansions of real numbers, Acta Math. Acad. Sci. Hungar. 11 (1960) 269-278

[13] G.Rauzy, Nombres Algébriques et substitutions, Bull. Soc. France 110 (1982) 147-178.

[14] K.Schmidt, On periodic expansions of Pisot numbers and Salem numbers, Bull. London Math. Soc. 12 (1980) 269–278

[15] W.P.Thurston, Groups, Tilings and Finite state automata, AMS Colloquium lectures, 1989.

Shigeki Akiyama

Dept. of Math., Fac. of Science
Niigata University,
Ikarashi-2 8050, Niigata
950-2181, JAPAN
E-mail: akiyama@math.sc.niigata-u.ac.jp
http://mathalg.ge.niigata-u.ac.jp/~akiyama
（このホームページからも、引用した拙著論文のコピーは入手可能である。）

有限 ROOT 系の THETA 級数に関連した ある組み合わせ論的等式について (AFFINE LIE 環の表現を背景として)

内藤 聡 (SATOSHI NAITO)

筑波大学・数学系

1. NONTWISTED AFFINE LIE 環と, その既約 HIGHEST WEIGHT 表現

この §1 では, nontwisted な affine Lie 環 $\hat{\mathfrak{g}}$ と, その既約 highest weight 表現 $\hat{L}(\Lambda)$ について, 記号の準備を兼ねながら幾つかの良く知られた事実を復習する. なお, 特に断らない限り, ベクトル空間は全て複素数体 $\mathbb{C}$ 上のものを考える事にする.

1.1. Nontwisted affine Lie 環. 先ず, $X = A, D, E$ と $N \in \mathbb{Z}_{\geq 1}$ に対して, $\mathfrak{g} := \mathfrak{g}(X_N)$ を X_N 型の (Cartan matrix を持つ) 有限次元複素単純 Lie 環, $\mathfrak{h}$ をその Cartan subalgebra とする ($N = \dim_{\mathbb{C}} \mathfrak{h}$ である). $\mathfrak{g}$ は次の様な root space 分解を持つ:

$$\mathfrak{g} = \left(\bigoplus_{\alpha \in \Delta_-} \mathfrak{g}_\alpha \right) \oplus \mathfrak{h} \oplus \left(\bigoplus_{\alpha \in \Delta_+} \mathfrak{g}_\alpha \right). \tag{1}$$

ここで, $\Delta_+ \subset \mathfrak{h}^* := \mathrm{Hom}_{\mathbb{C}}(\mathfrak{h}, \mathbb{C})$ は positive root の全体, $\Delta_- = -\Delta_+$ は negative root の全体であり, $\mathfrak{g}_\alpha$ は root $\alpha \in \Delta = \Delta_- \sqcup \Delta_+$ に対応する root space (この場合は, 全て 1 次元) である. そして, $\Pi = \{\alpha_i\}_{i=1}^N$ を simple root の全体, $Q := \sum_{i=1}^N \mathbb{Z}\alpha_i$ を ($\mathfrak{g}$ の) root lattice とする. 非常に良く知られている事であるが, $\alpha_1, \ldots, \alpha_N \in \mathfrak{h}^*$ は $\mathbb{C}$ 上で一次独立であり, しかも $\Delta_+ \subset \sum_{i=1}^N \mathbb{Z}_{\geq 0}\alpha_i$ となっている.

又, $(\cdot|\cdot)$ を $\mathfrak{g}$ 上の Killing form (非退化な対称双一次形式で不変: $([x,y]|z) = (x|[y,z])$, $x, y, z \in \mathfrak{g}$, なもの) とし, これの $\mathfrak{h}$ への制限が $\mathfrak{h}^*$ 上に誘導する非退化対称双一次形式も同じ記号 $(\cdot|\cdot)$ で表す. 但し, 以下では常に, 全ての (long) root α に対して $(\alpha|\alpha) = 2$ となる様に Killing form $(\cdot|\cdot)$ を normalize しておくものとする. ($\mathfrak{g}$ が A, D, E 型なので, 全ての root $\alpha \in \Delta$ の長さ $(\alpha|\alpha)$ は等しい.)

さて, $\hat{\mathfrak{g}} := \mathfrak{g}(X_N^{(1)}) = \hat{\mathcal{L}}(\mathfrak{g}) = (\mathbb{C}[t, t^{-1}] \otimes_{\mathbb{C}} \mathfrak{g}) \oplus \mathbb{C}c \oplus \mathbb{C}d$ を $X_N^{(1)}$ 型の (generalized Cartan matrix を持つ) nontwisted affine Lie 環, $\hat{\mathfrak{h}} := \mathfrak{h} \oplus \mathbb{C}c \oplus \mathbb{C}d$ をその Cartan

subalgebra とする. affine Lie 環 $\hat{\mathfrak{g}}$ の Lie 環としての構造は, 次の交換関係により定まる:

$$\begin{cases} [t^m \otimes x, t^n \otimes y] = t^{m+n} \otimes [x,y] + m\delta_{m+n,0}(x|y)c, \quad x,y \in \mathfrak{g},\ m,n \in \mathbb{Z}; \\ [c, \hat{\mathfrak{g}}] = 0; \\ [d, t^m \otimes x] = mt^m \otimes x, \quad x \in \mathfrak{g},\ m \in \mathbb{Z}. \end{cases} \tag{2}$$

この時 $\hat{\mathfrak{g}}$ は次の様な root space 分解を持つ:

$$\hat{\mathfrak{g}} = \left(\bigoplus_{\gamma \in \hat{\Delta}_-} \hat{\mathfrak{g}}_\gamma \right) \oplus \hat{\mathfrak{h}} \oplus \left(\bigoplus_{\gamma \in \hat{\Delta}_+} \hat{\mathfrak{g}}_\gamma \right). \tag{3}$$

ここで, $\hat{\Delta}_+ = \{j\delta \mid j \in \mathbb{Z}_{\geq 1}\} \sqcup \{j\delta + \alpha \mid j \in \mathbb{Z}_{\geq 1}, \alpha \in \Delta\} \sqcup \Delta_+$ は positive root の全体, $\hat{\Delta}_- = -\hat{\Delta}_+$ は negative root の全体であり, $\hat{\mathfrak{g}}_\gamma$ は root $\gamma \in \hat{\Delta} = \hat{\Delta}_- \sqcup \hat{\Delta}_+$ に対応する root space である. 但し, $\delta \in (\hat{\mathfrak{h}})^*$ は *null root* と呼ばれる元で, $\delta(\mathfrak{h} \oplus \mathbb{C}c) := 0$, $\delta(d) := 1$ により定義される. 各 root space $\hat{\mathfrak{g}}_\gamma$ は具体的には,

$$\hat{\mathfrak{g}}_{j\delta} = t^j \otimes \mathfrak{h}, \quad \hat{\mathfrak{g}}_{j\delta+\alpha} = t^j \otimes \mathfrak{g}_\alpha, \quad j \in \mathbb{Z}, \alpha \in \Delta \tag{4}$$

と書ける. そして simple root の全体を $\hat{\Pi} = \{\alpha_0 := \delta - \theta, \alpha_1, \ldots, \alpha_N\} \subset (\hat{\mathfrak{h}})^*$ とすれば ($\theta \in \Delta_+$ は *highest root* であり, $\theta, \alpha_1, \ldots, \alpha_n \in \mathfrak{h}^* \hookrightarrow (\hat{\mathfrak{h}})^*$ とみなしている), これらは $\mathbb{C}$ 上で一次独立であって, しかも $\hat{\Delta}_+ \subset \sum_{i=0}^N \mathbb{Z}_{\geq 0}\alpha_i$ となっている.

又, $\mathfrak{g}$ 上の normalized Killing form $(\cdot|\cdot)$ は, 次の様にして $\hat{\mathfrak{g}}$ 全体の上の不変な非退化対称双一次形式 $(\cdot|\cdot)$ に拡張される:

$$\begin{cases} (t^m \otimes x | t^n \otimes y) = \delta_{m+n,0}(x|y), \quad x,y \in \mathfrak{g},\ m,n \in \mathbb{Z}; \\ (\mathbb{C}c \oplus \mathbb{C}d | \mathbb{C}[t,t^{-1}] \otimes_{\mathbb{C}} \mathfrak{g}) = 0; \\ (c|c) = (d|d) = 0; \\ (c|d) = 1. \end{cases} \tag{5}$$

この $(\cdot|\cdot)$ の $\hat{\mathfrak{h}}$ への制限が $(\hat{\mathfrak{h}})^*$ 上に誘導する非退化対称双一次形式も, 同じ記号 $(\cdot|\cdot)$ で表す事にする. この時, 全ての $\alpha \in \Delta \subset \mathfrak{h}^* \hookrightarrow (\hat{\mathfrak{h}})^*$ に対して $(\alpha|\alpha) = 2$ である事に注意する.

1.2. $\hat{\mathfrak{g}}$ の既約 highest weight 表現. ここでは affine Lie 環 $\hat{\mathfrak{g}}$ の既約 highest weight 表現を考える. dominant integral weight $\Lambda \in \hat{P}_+ := \{\Lambda \in (\hat{\mathfrak{h}})^* \mid (\Lambda|\alpha_i) \in \mathbb{Z}_{\geq 0},\ 0 \leq i \leq N\}$ に対して, この Λ を highest weight とする $\hat{\mathfrak{g}}$ の 既約 highest weight 表現を

$\hat{L}(\Lambda)$ とする. これは, 以下の条件を満たす Lie 環 $\hat{\mathfrak{g}}$ の表現 (highest weight 表現) であって, 既約なものとして一意的に定まる:

(a) weight Λ を持つ nonzero weight vector $v_\Lambda \in \hat{L}(\Lambda)$ で, 全ての positive root $\gamma \in \hat{\Delta}_+$ に対して $\hat{\mathfrak{g}}_\gamma v_\Lambda = 0$ なるもの (highest weight vector) が存在する.

(b) $U(\hat{\mathfrak{g}})$ を Lie 環 $\hat{\mathfrak{g}}$ の universal enveloping algebra とする時, $U(\hat{\mathfrak{g}})v_\Lambda = \hat{L}(\Lambda)$ となっている (即ち, $\hat{L}(\Lambda)$ は $\hat{\mathfrak{g}}$-加群として v_Λ により生成される).

以下では dominant integral weight として, *basic fundamental weight* $\Lambda_0 \in (\hat{\mathfrak{h}})^*$ を取る事にする: $\Lambda_0(\mathfrak{h}) := 0$, $\Lambda_0(c) := 1$, $\Lambda_0(d) := 0$. この時の $\hat{\mathfrak{g}}$ の既約 highest weight 表現 $V := \hat{L}(\Lambda_0)$ は basic 表現と呼ばれ, その具体的な構成 (例えば, Frenkel-Kac の構成 [FK]) や, 指標公式 (Weyl-Kac の指標公式 [K4]) 等は良く知られている. それらの中で, 後に必要となる事実を幾つか説明する事にする.

先ず $d \in \hat{\mathfrak{g}}$ を用いて, basic 表現 $V = \hat{L}(\Lambda_0)$ に次の様な $\mathbb{Z}$-次数付け (basic gradation) を行う:

$$V = \bigoplus_{m \in \mathbb{Z}_{\geq 0}} V_m, \quad V_m := \{v \in V \mid dv = -mv\}. \tag{6}$$

この時, 各 $m \in \mathbb{Z}_{\geq 0}$ について V_m は有限次元である事が分かる。そこで, この $\dim_{\mathbb{C}} V_m$ の母関数 (graded dimension)

$$f(q) := \dim_q V = \sum_{m \geq 0} (\dim_{\mathbb{C}} V_m)\, q^m \tag{7}$$

を考える事が出来る. この $f(q)$ に関しては, Kac の結果として次の事実が知られている ([K4] 参照).

Fact 1. *basic* 表現 $\hat{L}(\Lambda_0) = V = \oplus_{m \geq 0} V_m$ の *graded dimension* $f(q) = \dim_q V$ は, 次の様に表せる.

$$f(q) = \frac{\Theta_Q(q)}{\phi(q)^N}. \tag{8}$$

ここで,

$$\Theta_Q(q) := \sum_{\alpha \in Q} q^{\frac{1}{2}(\alpha|\alpha)} \tag{9}$$

は $\mathfrak{g}$ の *root lattice* Q の *theta* 級数であり, $\phi(q) := \prod_{n=1}^{\infty}(1-q^n)$, $N = \dim_{\mathbb{C}} \mathfrak{h}$ である. 特に, $f(q)$ は複素数 $q \in \mathbb{C}$ の関数として $|q| < 1$ で (広義一様) 絶対収束している正則関数である.

Remark 1. Q は even lattice である (即ち, 全ての $\alpha \in Q$ に対して $(\alpha|\alpha) \in 2\mathbb{Z}$ である) 事に注意する.

1.3. $\mathfrak{g}$ の表現としての V の既約分解. 交換関係 (2) の $[d, t^0 \otimes \mathfrak{g}] = 0$ から, $V = \oplus_{m \geq 0} V_m$ の各斉次成分 V_m は $\mathfrak{g}$ の作用で不変 ($\mathfrak{g} V_m \subset V_m$) である事が分かる ($\mathfrak{g}$ は $t^0 \otimes \mathfrak{g} \subset \hat{\mathfrak{g}}$ と同一視出来る). この時, 各 V_m は有限次元なので, 有限次元複素単純 Lie 環 $\mathfrak{g}$ の表現として ($\mathfrak{g}$ の) 有限次元既約 highest weight 表現 $L(\lambda)$ 達の有限個の直和に分解する事が分かる. ここで, $L(\lambda)$ は dominant integral weight $\lambda \in P_+ := \{\lambda \in \mathfrak{h}^* \mid (\lambda|\alpha_i) \in \mathbb{Z}_{\geq 0},\ 1 \leq i \leq N\}$ を highest weight とする $\mathfrak{g}$ の既約 highest weight 表現 (従って, 必然的に有限次元) である. そこで, その重複度を $\Phi(\Lambda_0, \lambda)_m \in \mathbb{Z}_{\geq 0}$ と書く事にする:

$$V_m = \bigoplus_{\lambda \in P_+} \Phi(\Lambda_0, \lambda)_m \, L(\lambda). \tag{10}$$

そして, この重複度の母関数

$$\Phi(\Lambda_0, \lambda)(q) := \sum_{m \geq 0} \Phi(\Lambda_0, \lambda)_m \, q^m \tag{11}$$

を考える事にする. この $\Phi(\Lambda_0, \lambda)(q)$ に関しても, 次の Kac の結果が知られている ([K4] 参照).

Fact 2. $\lambda \in P_+$ とする. この時, 重複度 $\Phi(\Lambda_0, \lambda)_m$ の母関数 $\Phi(\Lambda_0, \lambda)(q)$ は, $\lambda \notin Q$ に対しては $\Phi(\Lambda_0, \lambda)(q) = 0$ で, そして $\lambda \in Q$ に対しては

$$\Phi(\Lambda_0, \lambda)(q) = \frac{q^{\frac{1}{2}(\lambda|\lambda)} \prod_{\alpha \in \Delta_+} \left(1 - q^{(\lambda+\rho|\alpha)}\right)}{\phi(q)^N} \tag{12}$$

で与えられる. ここで $\rho = \frac{1}{2} \sum_{\alpha \in \Delta_+} \alpha$ である.

Remark 2. $\mathfrak{g}$ は有限次元 Lie 環なので Δ_+ は有限集合であり, 従って上の Fact 2 における積 $\prod_{\alpha \in \Delta_+}$, 及び和 $\sum_{\alpha \in \Delta_+}$ はそれぞれ有限積, 有限和である.

2. THETA 級数 $\Theta_Q(q)$ に関するある等式

この §2 では, A_N, D_N, E_6, E_7, E_8 型の root lattice Q の theta 級数 $\Theta_Q(q)$ に関するある等式を, §1 で説明した諸結果から導く. 初めに断っておかなければならないが, この結果は §1 の Fact 1, 2 から直ちに導かれるものであるので, ほぼ同値な等式が幾つか Kac 自身によって既に発見されている. その一つは [K2] の Proposition 2 の後の Remark (d) にある等式であり, もう一つは [KT] の Remark 5.2 にある等式

である. 但し, 後で §4 において説明する様に, この等式は Q が B_l, C_l, F_4, G_2 型の有限次元複素単純 Lie 環 $\mathfrak{g}$ の root lattice である場合にも, そのままの形で成り立つ事が示せる. これらの場合については, 少なくとも上記の文献では触れられていない様である.

Proposition 1. *Q を A_N, D_N, E_6, E_7, E_8 型の有限次元複素単純 Lie 環 $\mathfrak{g}$ の root lattice, $(\cdot|\cdot)$ を $\mathfrak{h}^*$ 上の normalized (全ての $\alpha \in \Delta$ に対して $(\alpha|\alpha) = 2$ である) Killing form とする. この時, Q の theta 級数 $\Theta_Q(q) = \sum_{\alpha \in Q} q^{\frac{(\alpha|\alpha)}{2}}$ に関して, 次の等式が成り立つ.*

$$\Theta_Q(q) = \sum_{\lambda \in P_+ \cap Q} d(\lambda)\, q^{\frac{1}{2}(\lambda|\lambda)} \prod_{\alpha \in \Delta_+} \left(1 - q^{(\lambda+\rho|\alpha)}\right). \tag{13}$$

但し dominant integral weight $\lambda \in P_+ \subset \mathfrak{h}^*$ に対して, $d(\lambda)$ は λ を highest weight とする $\mathfrak{g}$ の有限次元既約 highest weight 表現 $L(\lambda)$ の次元 $\dim_{\mathbb{C}} L(\lambda)$ を表す.

Remark 3. 上の等式 (13) は, 複素変数 $q \in \mathbb{C}$ の正則関数に関する等式としても $|q| < 1$ において意味を持つ.

Remark 4. 上の Proposition 1 における $d(\lambda)$ は, 有名な Weyl の次元公式により Killing form $(\cdot|\cdot)$ を用いて,

$$d(\lambda) = \prod_{\alpha \in \Delta_+} \frac{(\lambda + \rho|\alpha)}{(\rho|\alpha)} \tag{14}$$

と表せる.

(Proposition 1 の証明.) $\hat{L}(\Lambda_0) = V = \oplus_{m \geq 0} V_m$ の graded dimension $f(q) = \dim_q V = \sum_{m \geq 0} (\dim_{\mathbb{C}} V_m)\, q^m$ を次の様に計算する. 先ず, Fact 2 より $\lambda \notin Q$ に対しては $\Phi(\Lambda_0, \lambda)_m = 0$ である事に注意すれば, (10) 式から直ちに

$$\dim_{\mathbb{C}} V_m = \sum_{\lambda \in P_+ \cap Q} d(\lambda)\, \Phi(\Lambda_0, \lambda)_m \tag{15}$$

を得る. 従って,

$$
\begin{aligned}
f(q) &= \sum_{m\geq 0} (\dim_{\mathbb{C}} V_m)\, q^m \\
&= \sum_{m\geq 0} \left(\sum_{\lambda\in P_+\cap Q} d(\lambda)\, \Phi(\Lambda_0,\lambda)_m \right) q^m && \text{“by (15)”} \\
&= \sum_{m\geq 0} \sum_{\lambda\in P_+\cap Q} d(\lambda)\, \Phi(\Lambda_0,\lambda)_m\, q^m \\
&= \sum_{\lambda\in P_+\cap Q} \sum_{m\geq 0} d(\lambda)\, \Phi(\Lambda_0,\lambda)_m\, q^m \\
&= \sum_{\lambda\in P_+\cap Q} d(\lambda) \left(\sum_{m\geq 0} \Phi(\Lambda_0,\lambda)_m\, q^m \right) \\
&= \sum_{\lambda\in P_+\cap Q} d(\lambda)\, \Phi(\Lambda_0,\lambda)(q) && \text{“by (11)”} \\
&= \sum_{\lambda\in P_+\cap Q} d(\lambda) \left(\frac{q^{\frac{1}{2}(\lambda|\lambda)} \prod_{\alpha\in\Delta_+} (1-q^{(\lambda+\rho|\alpha)})}{\phi(q)^N} \right) && \text{“by (12)”} \\
&= \phi(q)^{-N} \sum_{\lambda\in P_+\cap Q} d(\lambda)\, q^{\frac{1}{2}(\lambda|\lambda)} \prod_{\alpha\in\Delta_+} \left(1-q^{(\lambda+\rho|\alpha)}\right)
\end{aligned}
$$

となる.

一方, Fact 1 により $f(q) = \phi(q)^{-N}\Theta_Q(q)$ であった. これら二通りの $f(q)$ の表示を比べる事により, Proposition 1 の等式が得られる. □

Remark 5. 上の証明における式変形は, q の形式的ベキ級数環におけるものと考えても良いが, 複素変数 $q\in\mathbb{C}$ の ($|q|<1$ における) 正則関数に関する計算としても正当化される.

3. Theta 級数 $\Theta_Q(q)$ の微分に関するある等式

この §3 では, affine Lie 環 $\hat{\mathfrak{g}}$ の basic 表現 $\hat{L}(\Lambda_0) = V = \oplus_{m\geq 0} V_m$ への, 有限次元 Lie 環 $\mathfrak{g}$ ($\hookrightarrow \hat{\mathfrak{g}}$) の Casimir operator Ω の作用を調べる事により, theta 級数 $\Theta_Q(q)$ の q に関する微分 (に q を掛けたもの) $q\frac{d}{dq}\Theta_Q(q)$ に関するある等式を導く.

3.1. $\mathfrak{g}$ の Casimir operator Ω. 先ず, 有限次元複素単純 Lie 環 $\mathfrak{g}$ の basis の組 $\{u_i\}_{i=1}^M$, $\{u^i\}_{i=1}^M$ で, $(u_i|u^j) = \delta_{ij}$, $1\leq i,j\leq M$, なるもの (Killing form $(\cdot|\cdot)$ に関する dual bases) を取る. ここで $M = \dim_{\mathbb{C}}\mathfrak{g}$ である. $\mathfrak{g}$ の Casimir operator Ω は,

universal enveloping algebra $U(\mathfrak{g})$ における次の元として定義される:

$$\Omega := \sum_{i=1}^{M} u_i u^i \in U(\mathfrak{g}). \tag{16}$$

Remark 6. Casimir operator $\Omega \in U(\mathfrak{g})$ は $\mathfrak{g}$ の dual bases の取り方によらない. 特に

$$\Omega = \sum_{i=1}^{M} u_i u^i = \sum_{i=1}^{M} u^i u_i \tag{17}$$

である.

Casimir operator $\Omega \in U(\mathfrak{g})$ は, 実は universal enveloping algebra $U(\mathfrak{g})$ の center $Z(U(\mathfrak{g}))$ の元であり, 従って $\mathfrak{g}$ の既約 highest weight 表現 $L(\lambda)$ 上に scalar $C_\lambda \in \mathbb{C}$ として作用する. さらに, この scalar C_λ は Killing form $(\cdot|\cdot)$ を使って

$$C_\lambda = (\lambda + 2\rho|\lambda) \tag{18}$$

と表せる ([K4] 参照).

§2 で述べた様に, basic gradation により次数付けをした basic 表現 $\hat{L}(\Lambda_0) = V = \oplus_{m\geq 0} V_m$ の (有限次元の) 斉次成分 V_m は, $\mathfrak{g}$ の作用により不変であったから, 当然 Casimir operator $\Omega \in U(\mathfrak{g})$ の作用でも不変である. そこで, この線型変換 $\Omega|_{V_m}$ の trace $\mathrm{Tr}(\Omega|_{V_m}) \in \mathbb{C}$ の母関数 (graded trace)

$$g(q) := \sum_{m\geq 0} \mathrm{Tr}(\Omega|_{V_m})\, q^m \tag{19}$$

を考える事が出来る. 後の §3.3 では, この graded trace $g(q)$ を二通りの方法で計算する.

3.2. $\hat{\mathfrak{g}}$ の Casimir operator $\hat{\Omega}$. ここでは affine Lie 環 $\hat{\mathfrak{g}}$ の Casimir operator $\hat{\Omega}$ の構成と性質について, 良く知られた幾つかの事実を復習する. この $\hat{\Omega}$ は, $\hat{\mathfrak{g}}$ が無限次元である為, もはや通常の universal enveloping algebra $U(\hat{\mathfrak{g}})$ の元とはなり得ない. それでも $U(\hat{\mathfrak{g}})$ の *restricted completion* と呼ばれるある種の完備化の元とみなす事が出来て, 次の様に表される ([K4] 参照):

$$\hat{\Omega} = \Omega + 2(c + h^\vee)d + 2\sum_{i=1}^{M}\sum_{n\geq 1} (t^{-n}\otimes u_i)(t^n \otimes u^i). \tag{20}$$

但し, $h^\vee$ は *dual Coxeter number* と呼ばれる scalar である.

Remark 7. 上の dual Coxeter number $h^\vee$ は, 次で与えられる:

$$h^\vee = \begin{cases} N+1 & \text{if } X_N = A_N, \\ 2N-2 & \text{if } X_N = D_N, \\ 12 & \text{if } X_N = E_6, \\ 18 & \text{if } X_N = E_7, \\ 30 & \text{if } X_N = E_8. \end{cases} \tag{21}$$

さらに, 上記の全ての場合に

$$M = \dim_{\mathbf{C}} \mathfrak{g} = N(1+h^\vee) \tag{22}$$

が成り立つ ([K4] 参照).

Casimir operator $\hat{\Omega}$ は $\hat{\mathfrak{g}}$ の既約 highest weight 表現 $\hat{L}(\Lambda)$ の上に作用させる事が出来て, しかもその作用は $\hat{\mathfrak{g}}$ の作用と可換である. 実際, $\hat{\Omega}$ は $\hat{L}(\Lambda)$ 上に scalar $(\Lambda+2\hat{\rho}|\Lambda)$ として作用する. ここで $\hat{\rho} \in (\hat{\mathfrak{h}})^*$ は, $(\hat{\rho}|\alpha_i) = 1$, $0 \le i \le N$, と $\hat{\rho}(d) = 0$ (従って $(\hat{\rho}|\Lambda_0) = 0$) により一意的に定まる元であり, $\hat{\rho} = \rho + h^\vee \Lambda_0$ と書ける.

3.3. Graded trace の計算.

これから graded trace $g(q) = \sum_{m \ge 0} \mathrm{Tr}(\Omega|_{V_m}) q^m$ の計算を行うのであるが, その前に簡単な補題を 3 つ準備しておく.

先ず, 次の補題は線型代数の (非常に) 簡単な演習問題である.

Lemma 1. 有限次元の線型空間 V, W と, それらの間の線型写像 $A: V \to W$, $B: W \to V$ があるとする. この時, 合成写像 $A \circ B: W \to W$ の trace $\mathrm{Tr}(AB)$ と合成写像 $B \circ A: V \to V$ の trace $\mathrm{Tr}(BA)$ は等しい.

Proof. V, W の基底を取って, 実際に $\mathrm{Tr}(AB)$ と $\mathrm{Tr}(BA)$ を書いてみれば明らかである. □

§1 において $\phi(q) = \prod_{n=1}^{\infty}(1-q^n)$ という $|q| < 1$ における (零にならない) 正則関数を導入したが, さらに次の $|q| < 1$ における正則関数を導入する事にする:

$$h(q) := \phi(q)^{-N}, \quad H(q) := \log(h(q)). \tag{23}$$

次の 2 つの補題は, 関数論を用いればほぼ明らかなものであるが, ここでは敢えて q の形式的ベキ級数環の中で証明しておく.

Lemma 2. $H(q)$ の q に関する微分について, 次が成り立つ.

$$q\frac{d}{dq}H(q) = N\sum_{n\geq 1} n\sum_{j\geq 1} q^{nj}. \tag{24}$$

Proof. 先ず

$$H(q) = \log(h(q)) = (-N)\sum_{n\geq 1}\log(1-q^n)$$

であるから, これを q について微分して q を掛ければ,

$$\begin{aligned} q\frac{d}{dq}H(q) &= N\sum_{n\geq 1}\frac{nq^n}{1-q^n} \\ &= N\sum_{n\geq 1} n\sum_{j\geq 1} q^{nj} \end{aligned} \tag{25}$$

を得る. □

Lemma 3. $h(q)$ と $H(q)$ の q に関する微分について, 次の関係が成り立つ.

$$\frac{d}{dq}h(q) = h(q)\cdot\frac{d}{dq}H(q). \tag{26}$$

Proof. 積の微分法則を用いて $h(q) = \prod_{n\geq 1}\{(1-q^n)^{-N}\}$ を q に関して微分すれば,

$$\begin{aligned} \frac{d}{dq}h(q) &= \sum_{j\geq 1}\prod_{\substack{n\geq 1\\ n\neq j}}(1-q^n)^{-N}\cdot N(1-q^j)^{-N-1}\cdot jq^{j-1} \\ &= \sum_{j\geq 1}\left((1-q^j)^{-N}\prod_{\substack{n\geq 1\\ n\neq j}}(1-q^n)^{-N}\right)\cdot N(1-q^j)^{-1}\cdot jq^{j-1} \\ &= \sum_{j\geq 1}\left(\prod_{n\geq 1}(1-q^n)^{-N}\right)\cdot N(1-q^j)^{-1}\cdot jq^{j-1} \\ &= \prod_{n\geq 1}(1-q^n)^{-N}\cdot N\sum_{j\geq 1}\frac{jq^{j-1}}{1-q^j} \\ &= h(q)\cdot\frac{d}{dq}H(q) \qquad \text{“by (25)”} \end{aligned}$$

を得る. □

ここで, affine Lie 環 $\hat{\mathfrak{g}}$ における交換関係 (2) から, $1\leq i\leq M$, $n\geq 1$ に対して ($(u^i|u_i)=1$ だから)

$$[t^n\otimes u^i, t^{-n}\otimes u_i] = t^0\otimes[u^i,u_i] + nc = 1\otimes[u^i,u_i] + nc \tag{27}$$

が成り立つ事を注意しておく.

さて, 次が我々の主定理である.

Theorem 1. Q を A_N, D_N, E_6, E_7, E_8 型の有限次元複素単純 *Lie* 環 $\mathfrak{g}$ の *root lattice*, $(\cdot|\cdot)$ を *Cartan subalgebra* の *dual* $\mathfrak{h}^*$ 上の *normalized* (全ての $\alpha \in \Delta$ に対して $(\alpha|\alpha) = 2$ である) *Killing form*, そして $\Theta_Q(q) = \sum_{\alpha \in Q} q^{\frac{(\alpha|\alpha)}{2}}$ を Q の *theta* 級数とする. この時, 次の等式が成り立つ.

$$2(1+h^\vee)\, q\frac{d}{dq}\Theta_Q(q) = \sum_{\lambda \in P_+ \cap Q} d(\lambda)(\lambda+2\rho|\lambda)\, q^{\frac{(\lambda|\lambda)}{2}} \prod_{\alpha \in \Delta_+} \left(1 - q^{(\lambda+\rho|\alpha)}\right). \quad (28)$$

但し, $h^\vee$ は *dual Coxeter number* であり, $\rho = \frac{1}{2}\sum_{\alpha \in \Delta_+} \alpha$, $d(\lambda) = \dim_{\mathbb{C}} L(\lambda)$ である.

Remark 8. 上の等式 (28) は, 複素変数 $q \in \mathbb{C}$ の正則関数に関する等式としても $|q| < 1$ において意味を持つ.

(Theorem 1 の証明.) §3.2 で述べた様に, affine Lie 環 $\hat{\mathfrak{g}}$ の Casimir operator $\hat{\Omega}$ は basic 表現 $V = \hat{L}(\Lambda_0)$ に scalar $(\Lambda_0+2\hat{\rho}|\Lambda_0)$ として作用する. ところが, $(\Lambda_0|\Lambda_0) = 0$, $(\hat{\rho}|\Lambda_0) = 0$ であるから, 実は $\hat{\Omega}$ は V 上に zero operator として作用する事になる. 一方, $\hat{\Omega}$ は universal enveloping algebra の完備化の元として, (20) 式の表示を持っていた. この表示において, c は $\hat{\mathfrak{g}}$ の center の元だから V 上に scalar $\Lambda_0(c) = 1$ として作用し, d は各斉次成分 V_m 上には scalar $-m$ として作用する. よって, V_m 上の作用素として

$$0 = \Omega|_{V_m} - 2(1+h^\vee)m\, I_{V_m} + 2\sum_{i=1}^{M}\sum_{n \geq 1} u_i(-n)u^i(n)|_{V_m}$$

が成り立つ. ここで $x \in \mathfrak{g}$, $n \in \mathbb{Z}$ に対して, $x(n) \in \mathrm{End}_{\mathbb{C}} V$ は $t^n \otimes x \in \hat{\mathfrak{g}}$ の定める basic 表現 $V = \hat{L}(\Lambda_0)$ 上の作用素を表している. 但し, 交換関係 (2) の $[d, t^n \otimes x] = nt^n \otimes x$ より, $x(n)V_m \subset V_{m-n}$ である事に注意する. 従って結局, 各 $m \geq 0$ に対して次が成り立つ事になる.

$$\mathrm{Tr}(\Omega|_{V_m}) = 2(1+h^\vee)m\,(\dim_{\mathbb{C}} V_m) - 2\sum_{i=1}^{M}\sum_{n \geq 1} \mathrm{Tr}(u_i(-n)u^i(n)|_{V_m}). \quad (29)$$

Claim 1. 各 $1 \leq i \leq M$, $n \geq 1$ に対して, $\mathrm{Tr}(u_i(-n)u^i(n)|_{V_m})$ は

$$\mathrm{Tr}(u_i(-n)u^i(n)|_{V_m}) = n\sum_{j \geq 1} \dim_{\mathbb{C}} V_{m-nj} \quad (30)$$

で与えられる．特に，この値は $1 \leq i \leq M$ によらない．但し，$m < 0$ に対しては $V_m := \{0\}$ と考えるものとする．

Claim 1 の証明は後で与える事にして，ここではこれを認めて Theorem 1 の証明を完成させる．(29) 式と Claim 1 の (30) 式より

$$\mathrm{Tr}(\Omega|_{V_m}) = 2(1+h^\vee)m(\dim_{\mathbf{C}} V_m) - 2M\sum_{n\geq 1} n \sum_{j\geq 1} \dim_{\mathbf{C}} V_{m-nj} \tag{31}$$

となるから，$\mathrm{Tr}(\Omega|_{V_m})$ の母関数 $g(q)$ は $f(q) = \sum_{m\geq 0}(\dim_{\mathbf{C}} V_m)\, q^m$ を用いて

$$\begin{aligned}
g(q) &= \sum_{m\geq 0} \mathrm{Tr}(\Omega|_{V_m})\, q^m \\
&= 2(1+h^\vee)\, q\frac{d}{dq}f(q) - 2M \sum_{m\geq 0}\left(\sum_{n\geq 1} n \sum_{j\geq 1} \dim_{\mathbf{C}} V_{m-nj}\right) q^m && \text{“by (31)”} \\
&= 2(1+h^\vee)\, q\frac{d}{dq}f(q) - 2M \sum_{m\geq 0}\sum_{\substack{n\geq 1\\ j\geq 1}} n(\dim_{\mathbf{C}} V_{m-nj})\, q^m \\
&= 2(1+h^\vee)\, q\frac{d}{dq}f(q) - 2M \sum_{\substack{n\geq 1\\ j\geq 1}}\sum_{m\geq 0} n(\dim_{\mathbf{C}} V_{m-nj})\, q^m \\
&= 2(1+h^\vee)\, q\frac{d}{dq}f(q) - 2M \sum_{\substack{n\geq 1\\ j\geq 1}}\sum_{m\geq 0} n(\dim_{\mathbf{C}} V_{m})\, q^{m+nj} \\
&= 2(1+h^\vee)\, q\frac{d}{dq}f(q) - 2M \sum_{m\geq 0}\sum_{\substack{n\geq 1\\ j\geq 1}} n(\dim_{\mathbf{C}} V_{m})\, q^{m+nj} \\
&= 2(1+h^\vee)\, q\frac{d}{dq}f(q) - 2M \left(\sum_{m\geq 0}(\dim_{\mathbf{C}} V_m)\, q^m\right)\cdot\left(\sum_{n\geq 1} n\sum_{j\geq 1} q^{nj}\right) \\
&= 2(1+h^\vee)\, q\frac{d}{dq}f(q) - 2M f(q)\cdot\frac{1}{N} q\frac{d}{dq}H(q) && \text{“by (24)”}
\end{aligned}$$

と表せる．ところで Remark 7 の (22) 式より，$M = \dim_{\mathbf{C}} \mathfrak{g} = N(1+h^\vee)$ であったから，

$$\begin{aligned}
g(q) &= 2q\left\{(1+h^\vee)\frac{d}{dq}f(q) - \frac{M}{N}\cdot f(q)\frac{d}{dq}H(q)\right\} \\
&= 2(1+h^\vee)\, q\left\{\frac{d}{dq}f(q) - f(q)\frac{d}{dq}H(q)\right\}
\end{aligned}$$

となる. 又, Fact 1 より $f(q) = h(q)\Theta_Q(q)$ であったから,

$$\begin{aligned}\frac{d}{dq}f(q) &= \Theta_Q(q)\frac{d}{dq}h(q) + h(q)\frac{d}{dq}\Theta_Q(q) \\ &= \Theta_Q(q)\left(h(q)\cdot\frac{d}{dq}H(q)\right) + h(q)\frac{d}{dq}\Theta_Q(q) \qquad \text{“by (26)”} \\ &= f(q)\frac{d}{dq}H(q) + h(q)\frac{d}{dq}\Theta_Q(q)\end{aligned}$$

となる. これらを合わせて, 結局

$$g(q) = h(q)\cdot 2(1+h^\vee)\, q\frac{d}{dq}\Theta_Q(q) \tag{32}$$

である事が分かった.

さてここで (10) 式と Fact 2 を思い出すと, 斉次成分 V_m は

$$V_m = \bigoplus_{\lambda\in P_+\cap Q} \Phi(\Lambda_0,\lambda)_m\, L(\lambda)$$

と, g の既約 highest weight 表現 $L(\lambda)$ 達の直和に分解していた. そこで, g の Casimir operator Ω は $L(\lambda)$ 上に scalar $C_\lambda = (\lambda+2\rho|\lambda)$ として作用する事に注意すれば, 各 $m \geq 0$ に対して

$$\mathrm{Tr}(\Omega|_{V_m}) = \sum_{\lambda\in P_+\cap Q} d(\lambda)(\lambda+2\rho|\lambda)\,\Phi(\Lambda_0,\lambda)_m \tag{33}$$

である事が分かる. 従って

$$\begin{aligned}g(q) &= \sum_{m\geq 0}\mathrm{Tr}(\Omega|_{V_m})q^m \\ &= \sum_{m\geq 0}\sum_{\lambda\in P_+\cap Q} d(\lambda)(\lambda+2\rho|\lambda)\,\Phi(\Lambda_0,\lambda)_m\, q^m \qquad \text{“by (33)”} \\ &= \sum_{\lambda\in P_+\cap Q} d(\lambda)(\lambda+2\rho|\lambda)\left(\sum_{m\geq 0}\Phi(\Lambda_0,\lambda)_m\, q^m\right) \\ &= \sum_{\lambda\in P_+\cap Q} d(\lambda)(\lambda+2\rho|\lambda)\,\Phi(\Lambda_0,\lambda)(q) \qquad \text{“by (11)”} \\ &= \sum_{\lambda\in P_+\cap Q} d(\lambda)(\lambda+2\rho|\lambda)\left(h(q)\,q^{\frac{(\lambda|\lambda)}{2}}\prod_{\alpha\in\Delta_+}(1-q^{(\lambda+\rho|\alpha)})\right) \qquad \text{“by (12)”} \\ &= h(q)\cdot\sum_{\lambda\in P_+\cap Q} d(\lambda)(\lambda+2\rho|\lambda)\,q^{\frac{(\lambda|\lambda)}{2}}\prod_{\alpha\in\Delta_+}\left(1-q^{(\lambda+\rho|\alpha)}\right)\end{aligned}$$

と表せる. この表示を先に得られた $g(q)$ の表示 (32) 式と比べる事により, Theorem 1 の等式が得られる. □

Remark 9. 上の証明における式変形は, q の形式的ベキ級数環におけるものであるが, 複素変数 $q \in \mathbb{C}$ の ($|q| < 1$ における) 正則関数に関する計算としても正当化される.

(Claim 1 の証明.) 先ず, 各 $1 \leq i \leq M$, $n \geq 1$ について,

$$u^i(n)\colon V_m \to V_{m-n}, \quad u_i(-n)\colon V_{m-n} \to V_m$$

であり, よって

$$u_i(-n) \circ u^i(n)\colon V_m \to V_m, \quad u^i(n) \circ u_i(-n)\colon V_{m-n} \to V_{m-n}$$

である事に注意する. 従って Lemma 1 より

$$\mathrm{Tr}(u_i(-n)u^i(n)|_{V_m}) = \mathrm{Tr}(u^i(n)u_i(-n)|_{V_{m-n}}) \tag{34}$$

である. 又

$$u^i(n)\colon V_{m-n} \to V_{m-2n}, \quad u_i(-n)\colon V_{m-2n} \to V_{m-n}$$

であり, よって

$$u_i(-n) \circ u^i(n)\colon V_{m-n} \to V_{m-n}$$

である事に注意すれば, 交換関係 (27) から

$$\mathrm{Tr}(u^i(n)u_i(-n)|_{V_{m-n}}) = \mathrm{Tr}(u_i(-n)u^i(n)|_{V_{m-n}}) + \mathrm{Tr}([u^i, u_i]|_{V_{m-n}}) + n\,\mathrm{Tr}(I_V|_{V_{m-n}})$$

が分かる. ここで, 再び Lemma 1 より

$$\begin{aligned}\mathrm{Tr}([u^i, u_i]|_{V_{m-n}}) &= \mathrm{Tr}(u^i|_{V_{m-n}} \circ u_i|_{V_{m-n}} - u_i|_{V_{m-n}} \circ u^i|_{V_{m-n}}) \\ &= \mathrm{Tr}(u^i|_{V_{m-n}} u_i|_{V_{m-n}}) - \mathrm{Tr}(u_i|_{V_{m-n}} u^i|_{V_{m-n}}) \\ &= 0\end{aligned}$$

であるから, 結局

$$\mathrm{Tr}(u^i(n)u_i(-n)|_{V_{m-n}}) = \mathrm{Tr}(u_i(-n)u^i(n)|_{V_{m-n}}) + n\,(\dim_{\mathbb{C}} V_{m-n}) \tag{35}$$

が分かった事になる. そこで, (34) 式と (35) 式を合わせる事により, 漸化式

$$\mathrm{Tr}(u_i(-n)u^i(n)|_{V_m}) = \mathrm{Tr}(u_i(-n)u^i(n)|_{V_{m-n}}) + n\,(\dim_{\mathbb{C}} V_{m-n})$$

を得る. この漸化式から, 十分大きい整数 j に対しては $V_{m-nj} = \{0\}$ である事に注意して,

$$\mathrm{Tr}(u_i(-n)u^i(n)|_{V_m}) = n\sum_{j\geq 1}\dim_{\mathbb{C}} V_{m-nj}$$

が導かれる. □

3.4. Example. 最も簡単な場合として, $\mathfrak{g}$ が A_2 型の 8 次元複素単純 Lie 環, 即ち

$$\mathfrak{g} = \mathfrak{sl}(3,\mathbb{C}) = \{X \in M(3,\mathbb{C}) \mid \mathrm{Tr}(X) = 0\}$$

である場合に, Theorem 1 の等式 (28) をより具体的に書き下してみる. この場合, Cartan subalgebra は

$$\mathfrak{h} = \{h = \mathrm{diag}(h_1,h_2,h_3) \mid h_i \in \mathbb{C}, 1 \leq i \leq 3,\ h_1+h_2+h_3 = 0\}$$

であり, simple root は $\alpha_1 = \lambda_1 - \lambda_2$, $\alpha_2 = \lambda_2 - \lambda_3$, そして root lattice は

$$Q = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2 = \{k\alpha_1 + m\alpha_2 \mid k,m \in \mathbb{Z}\}$$

である. 但し, $\lambda_1,\lambda_2,\lambda_3$ は $h = \mathrm{diag}(h_1,h_2,h_3) \in \mathfrak{h}$ に対して $\lambda_i(h) := h_i$ で定まる $\mathfrak{h}^*$ の元である. なお, これらの $\lambda_1,\lambda_2,\lambda_3$ は一次独立ではなく, $\lambda_1+\lambda_2+\lambda_3 = 0$ である事に注意する. さらに, positive root は $\Delta_+ = \{\alpha_1,\alpha_2,\alpha_1+\alpha_2\}$ なので, $\rho = \alpha_1+\alpha_2$ である. そして Remark 7 の (21) 式より dual Coxeter number は $h^\vee = 3$ で与えられる.

又, Killing form $(\cdot|\cdot)$ に関しては

$$(\alpha_1|\alpha_1) = (\alpha_2|\alpha_2) = 2, \quad (\alpha_1|\alpha_2) = -1$$

であり, よって $\lambda = k\alpha_1 + m\alpha_2 \in Q$ について

$$(\lambda+\rho|\alpha_1) = 2k-m+1, \quad (\lambda+\rho|\alpha_2) = -k+2m+1, \quad (\lambda+\rho|\alpha_1+\alpha_2) = k+m+2,$$

$$\frac{(\lambda|\lambda)}{2} = k^2 - km + m^2, \quad (\rho|\lambda) = k+m$$

である. 特に $\lambda = k\alpha_1 + m\alpha_2 \in Q$ に対して, $\lambda \in P_+ \cap Q$ である為の条件は $2k - m \geq 0$ かつ $2m - k \geq 0$ (この時, 必然的に $k, m \geq 0$) である:

$$P_+ \cap Q = \{k\alpha_1 + m\alpha_2 \mid 2k \geq m \geq 0,\ 2m \geq k \geq 0,\ k, m \in \mathbb{Z}\}.$$

そして $\lambda = k\alpha_1 + m\alpha_2 \in P_+ \cap Q$ に対する $d(\lambda) = \dim_{\mathbb{C}} L(\lambda)$ は (14) 式より

$$d(\lambda) = \frac{1}{2}(2k - m + 1)(2m - k + 1)(k + m + 2)$$

となる.

以上を考慮すれば, Theorem 1 の等式 (28) は次の様に書ける:

$$\begin{aligned} &8 \cdot \sum_{k,m \in \mathbb{Z}} (k^2 - km + m^2)\, q^{k^2 - km + m^2} \\ &= \sum_{\substack{2k \geq m \geq 0 \\ 2m \geq k \geq 0 \\ k,m \in \mathbb{Z}}} (2k - m + 1)(2m - k + 1)(k + m + 2)(k^2 - km + m^2 + k + m) \\ &\qquad \times q^{k^2 - km + m^2}(1 - q^{2k - m + 1})(1 - q^{2m - k + 1})(1 - q^{k + m + 2}). \end{aligned}$$

4. Twisted affine Lie 環の場合

この §4 では, B_l, C_l, F_4, G_2 型の有限次元複素単純 Lie 環の root lattice に対しても, やはり Proposition 1, Theorem 1 と同様の結果が成り立つ事を簡単に説明する.

4.1. Twisted affine Lie 環. ここでは twisted affine Lie 環について, 良く知られている幾つかの事実を [K4] 及び [W] に従って復習する. 先ず, $X_N = A_{2l-1}$ $(l \geq 3)$, D_{l+1} $(l \geq 2)$, E_6, D_4 に対して, $\mathfrak{g} := \mathfrak{g}(X_N)$ を X_N 型の有限次元複素単純 Lie 環, $\mathfrak{h}$ をその Cartan subalgebra, $(\cdot|\cdot)$ を $\mathfrak{h}^*$ 上の (全ての root $\alpha \in \Delta$ について $(\alpha|\alpha) = 2$ である様に) normalize された Killing form とする. そして μ を, X_N 型の Cartan matrix $A := A(X_N) = (a_{ij})_{i,j=1}^N$ (の Dynkin 図形) の *diagram automorphism* とする. 即ち μ は添字集合 $\{1, 2, \ldots, N\}$ の置換で, 条件

$$a_{\mu(i),\mu(j)} = a_{ij}, \quad 1 \leq i, j \leq N \tag{36}$$

を満たすものとする.

Remark 10. $X_N = D_4$ の場合には, diagram automorphism μ は 2 つ (同値なものが) あり, それらの位数は 3 である. その他の場合には, diagram automorphism μ は 1 つだけであり, その位数は 2 である.

容易に分かる様に, この diagram automorphism μ は, $\mathfrak{g}$ の Lie 環としての自己同型写像 $\mu: \mathfrak{g} \to \mathfrak{g}$ で, $\mu(\mathfrak{h}) = \mathfrak{h}$ なるものに自然に拡張される. この時 Killing form $(\cdot|\cdot)$ は μ-不変:

$$(\mu(x)|\mu(y)) = (x|y), \quad x, y \in \mathfrak{g} \tag{37}$$

である事を注意しておく. この μ の位数を r とすると ($r = 2, 3$ である), $\mathfrak{g}$ は次の様に μ の固有空間に分解する:

$$\mathfrak{g} = \bigoplus_{k \in \mathbb{Z}/r\mathbb{Z}} \mathfrak{g}_k, \quad \mathfrak{g}_k := \{x \in \mathfrak{g} \mid \mu(x) = \epsilon^k x\}. \tag{38}$$

ここで $\epsilon := \exp(\frac{2\pi\sqrt{-1}}{r}) \in \mathbb{C}$ である. 又, $\mu(\mathfrak{h}) = \mathfrak{h}$ である事から, 当然 $\mathfrak{h}$ も

$$\mathfrak{h} = \bigoplus_{k \in \mathbb{Z}/r\mathbb{Z}} \mathfrak{h}_k, \quad \mathfrak{h}_k := \mathfrak{g}_k \cap \mathfrak{h} \tag{39}$$

と分解する. さらに, 各 $\mathfrak{g}_k$ は $\mathfrak{h}_0$ の adjoint action により

$$\mathfrak{g}_k = \mathfrak{h}_k \oplus \bigoplus_{\alpha \in \Delta_k} \mathfrak{g}_{k,\alpha} \tag{40}$$

と, $\mathfrak{h}_0$ に関する weight space に分解する.

以下では, 整数 $i \in \mathbb{Z}$ に対して, 剰余環 $\mathbb{Z}/r\mathbb{Z}$ において i の属する剰余類を $\bar{i} := i + r\mathbb{Z} \in \mathbb{Z}/r\mathbb{Z}$ と書く事にする. μ は $\mathfrak{g}$ の Lie 環としての自己同型写像なので, $i, j \in \mathbb{Z}$ に対して

$$[\mathfrak{g}_{\bar{i}}, \mathfrak{g}_{\bar{j}}] \subset \mathfrak{g}_{\overline{i+j}} \tag{41}$$

である. 特に $\mathfrak{g}_{\bar{0}}$ は $\mathfrak{g}$ の部分 Lie 環で, $\mathfrak{g}_{\bar{i}}$ と $\mathfrak{g}_{\overline{-i}}$ は $\mathfrak{g}_{\bar{0}}$ の adjoint action に関して同値な表現空間となっている. さらに, 実は $\mathfrak{g}_{\bar{0}}$ は有限次元複素単純 Lie 環 $\mathfrak{g}(Y_L)$ であり, その型 Y_L は次の通りである:

$$Y_L = \begin{cases} C_l & \text{if } X_N = A_{2l-1}, \ r = 2, \\ B_l & \text{if } X_N = D_{l+1}, \ r = 2, \\ F_4 & \text{if } X_N = E_6, \ r = 2, \\ G_2 & \text{if } X_N = D_4, \ r = 3. \end{cases} \tag{42}$$

又, Killing form $(\cdot|\cdot)$ が μ-不変である事から, $i,j \in \mathbb{Z}$ に対して, $\bar{i}+\bar{j} \neq \bar{0} \in \mathbb{Z}/r\mathbb{Z}$ の時は $(\mathfrak{g}_i|\mathfrak{g}_j) = 0$ であり, $\bar{i}+\bar{j} = \bar{0} \in \mathbb{Z}/r\mathbb{Z}$ の時は pairing $(\cdot|\cdot)\colon \mathfrak{g}_i \times \mathfrak{g}_j \to \mathbb{C}$, $(\cdot|\cdot)\colon \mathfrak{h}_i \times \mathfrak{h}_j \to \mathbb{C}$ は共に非退化である事が分かる.

それでは, $X_N^{(r)} = A_{2l-1}^{(2)}, D_{l+1}^{(2)}, E_6^{(2)}, D_4^{(3)}$ に対して. $X_N^{(r)}$ 型の (generalized Cartan matrix を持つ) twisted affine Lie 環 $\hat{\mathfrak{g}} := \mathfrak{g}(X_N^{(r)}) = \hat{\mathcal{L}}(\mathfrak{g},\mu,r)$ を導入しよう. ここで, $X_N^{(r)}$ 型の generalized Cartan matrix は $(l+1)\times(l+1)$-行列である事に注意しなければならない. 但し, $X_N^{(r)} = E_6^{(2)}$ の場合は $l=4$, $X_N^{(r)} = D_4^{(3)}$ の場合は $l=2$ とする. (詳しくは [K4] を参照されたい.)

しかし twisted affine Lie 環 $\hat{\mathfrak{g}}$ を導入する前に, 記号の混乱を避ける為, $X_N^{(1)}$ 型の nontwisted affine Lie 環 $\mathfrak{g}(X_N^{(1)})$ に対する記号を §1 から §3 までにおけるものから少し変更しておく必要がある. そこでこの §4 においては, $X_N^{(1)}$ 型の nontwisted affine Lie 環を $\tilde{\mathfrak{g}} = \mathfrak{g}(X_N^{(1)}) = \tilde{\mathcal{L}}(\mathfrak{g}) = (\mathbb{C}[t,t^{-1}]\otimes_{\mathbb{C}}\mathfrak{g})\oplus\mathbb{C}c'\oplus\mathbb{C}d'$, その Cartan subalgebra を $\tilde{\mathfrak{h}} = \mathfrak{h}\oplus\mathbb{C}c'\oplus\mathbb{C}d'$ と書く事にする.

さて, $X_N^{(r)}$ 型の twisted affine Lie 環 $\hat{\mathfrak{g}} := \mathfrak{g}(X_N^{(r)}) = \hat{\mathcal{L}}(\mathfrak{g},\mu,r)$ は, $\tilde{\mathfrak{g}}$ の部分 Lie 環として次の様に定義される:

$$\hat{\mathcal{L}}(\mathfrak{g},\mu,r) := \left(\bigoplus_{j\in\mathbb{Z}} t^j\otimes\mathfrak{g}_{\bar{j}}\right)\oplus\mathbb{C}c\oplus\mathbb{C}d. \tag{43}$$

但し, $c := rc'$, $d := d'$ である. $\hat{\mathfrak{g}}$ の Cartan subalgebra は $\hat{\mathfrak{h}} := \mathfrak{h}_{\bar{0}}\oplus\mathbb{C}c\oplus\mathbb{C}d$ であり, $\hat{\mathfrak{h}}$ に関する positive root の全体 $\hat{\Delta}_+ \subset (\hat{\mathfrak{h}})^*$ は

$$\hat{\Delta}_+ = \{j\delta \mid j\in\mathbb{Z}_{\geq 1}\}\sqcup\{j\delta+\alpha \mid j\in\mathbb{Z}_{\geq 1}, \alpha\in\Delta_{\bar{j}}\}\sqcup(\Delta_{\bar{0}})_+ \tag{44}$$

である. ここで $\delta\in(\mathfrak{h}_{\bar{0}})^*$ は, $\tilde{\mathfrak{g}}$ の null root $\delta\in(\tilde{\mathfrak{h}})^*$ を $\hat{\mathfrak{h}}\subset\tilde{\mathfrak{h}}$ に制限したものである. 各 root $\gamma\in\hat{\Delta}_+$ に対応する root space $\hat{\mathfrak{g}}_\gamma$ は

$$\hat{\mathfrak{g}}_{j\delta} = t^j\otimes\mathfrak{g}_{\bar{j},0},\quad \hat{\mathfrak{g}}_{j\delta+\alpha} = t^j\otimes\mathfrak{g}_{\bar{j},\alpha},\quad j\in\mathbb{Z},\ \alpha\in\Delta_{\bar{j}} \tag{45}$$

と書ける. 又, $\hat{\mathfrak{g}}$ の simple root の全体を $\hat{\Pi} = \{\alpha_i\}_{i=0}^l \subset \hat{\Delta}_+$ としておく. (本来なら $\{\alpha_i\}_{i=0}^l$ を $\mathfrak{g}$ の simple roots からどの様に定めるかをきちんと説明すべきなのだが, 少し面倒なのでこの様な書き方に止めた.)

(42) 式にある様に $\mathfrak{g}_{\bar{0}}$ は有限次元複素単純 Lie 環 $\mathfrak{g}(Y_L)$ であったが, 一方でこの $\mathfrak{g}_{\bar{0}}$ は $t^0\otimes\mathfrak{g}_{\bar{0}}$ と同一視する事により twisted affine Lie 環 $\hat{\mathfrak{g}} = \mathfrak{g}(X_N^{(r)})$ の部分 Lie 環

ともみなせる. 実はこの時 Cartan matrix Y_L は, generalized Cartan matrix $X_N^{(r)}$ から添字 0 に対応する行と列を取り除いて得られる principal submatrix であって, $\mathfrak{g}(Y_L) = \mathfrak{g}_{\bar{0}} \cong t^0 \otimes \mathfrak{g}_{\bar{0}}$ は $\mathfrak{g}(X_N^{(r)}) = \hat{\mathfrak{g}}$ に "自然に埋め込まれた" 部分 Lie 環になっている. 特に $\mathfrak{g}(Y_L)$ の Cartan subalgebra は $\mathfrak{h}_{\bar{0}} \subset \hat{\mathfrak{h}}$, root の全体は $\Delta_{\bar{0}} \subset (\mathfrak{h}_{\bar{0}})^*$, そして root lattice は $Q := \sum_{i=1}^{l} \mathbb{Z}\alpha_i \subset (\mathfrak{h}_{\bar{0}})^*$ と見なせる.

又, $\mathfrak{g}$ 上の normalized Killing form $(\cdot|\cdot)$ から, 次の様にして $\hat{\mathfrak{g}}$ 全体の上の不変な非退化対称双一次形式 $(\cdot|\cdot)^\wedge$ が定義される:

$$\begin{cases} (t^i \otimes x|t^j \otimes y)^\wedge = r^{-1}\delta_{i+j,0}(x|y), \quad i,j \in \mathbb{Z}, \ x \in \mathfrak{g}_{\bar{i}}, \ y \in \mathfrak{g}_{\bar{j}}; \\ (\mathbb{C}c \oplus \mathbb{C}d|t^j \otimes \mathfrak{g}_{\bar{j}})^\wedge = 0, \quad j \in \mathbb{Z}, \ x \in \mathfrak{g}_{\bar{j}}; \\ (c|c)^\wedge = (d|d)^\wedge = 0; \\ (c|d)^\wedge = 1. \end{cases} \tag{46}$$

さて, $\mathfrak{g}_{\bar{0}} = \mathfrak{g}(Y_L)$ は $\mathfrak{g} = \mathfrak{g}(X_N)$ の部分 Lie 環であると同時に, twisted affine Lie 環 $\hat{\mathfrak{g}} = \mathfrak{g}(X_N^{(r)})$ の部分 Lie 環でもあった. この時, 上の定義から分かる様に, $x, y \in \mathfrak{g}_{\bar{0}} = \mathfrak{g}(Y_L)$ に対して

$$(x|y)^\wedge = r^{-1}(x|y) \tag{47}$$

という関係がある. さらに, 有限次元複素単純 Lie 環 $\mathfrak{g}(Y_L)$ 上の Killing form $\langle \cdot, \cdot \rangle$ を全ての long root $\alpha \in (\Delta_{\bar{0}})_l$ に対して $\langle \alpha, \alpha \rangle = 2$ となる様に normalize したものは, $\mathfrak{g}$ 上の normalized Killing form $(\cdot|\cdot)$ を $\mathfrak{g}_{\bar{0}} = \mathfrak{g}(Y_L)$ に制限したものと一致する:

$$\langle x, y \rangle = (x|y), \quad x, y \in \mathfrak{g}_{\bar{0}} = \mathfrak{g}(Y_L). \tag{48}$$

よって以下では, 有限次元複素単純 Lie 環 $\mathfrak{g}(Y_L)$ 上の normalized Killing form をも, 記号 $(\cdot|\cdot)$ で表す事にする.

最後に, twisted affine Lie 環 $\hat{\mathfrak{g}}$ の Casimir operator $\hat{\Omega}$ の構成について述べておく. この $\hat{\Omega}$ は, $\hat{\mathfrak{g}}$ の universal enveloping algebra $U(\hat{\mathfrak{g}})$ の完備化の元として次の様に表される:

$$\hat{\Omega} = r\Omega + 2(c + h^\vee)d + 2r \sum_{k \in \mathbb{Z}/r\mathbb{Z}} \sum_{\substack{n \geq 1 \\ n = k}} \sum_{i=1}^{\dim \mathfrak{g}_k} (t^{-n} \otimes u^{(k)i})(t^n \otimes u_i^{(k)}). \tag{49}$$

ここで, $\Omega \in Z(U(\mathfrak{g}_{\bar{0}}))$ は Y_L 型の有限次元複素単純 Lie 環 $\mathfrak{g}_{\bar{0}} = \mathfrak{g}(Y_L)$ の Casimir operator であり, 各 $k \in \mathbb{Z}/r\mathbb{Z}$ に対して $\{u_i^{(k)} \mid 1 \leq i \leq \dim_{\mathbb{C}} \mathfrak{g}_k\}$ と $\{u^{(k)i} \mid 1 \leq i \leq$

$\dim_{\mathbb{C}} \mathfrak{g}_k\}$ は, それぞれ $\mathfrak{h}_{\bar{0}}$ の adjoint action に関する weight vector から成る $\mathfrak{g}_k$ と $\mathfrak{g}_{-k}$ の basis で,

$$\begin{cases} (u_i^{(k)}|u^{(k)j}) = \delta_{ij}, \quad 1 \le i,j \le \dim_{\mathbb{C}} \mathfrak{g}_k \\ \sum_{i=1}^{\dim \mathfrak{g}_k} [u_i^{(k)}, u^{(k)i}] = 0 \in \mathfrak{h}_{\bar{0}} \end{cases} \tag{50}$$

なるものである. そして $h^\vee$ は 次で与えられる dual Coxeter number である:

$$h^\vee = \begin{cases} 2l & \text{if } X_N^{(r)} = A_{2l-1}^{(2)}, \\ 2l & \text{if } X_N^{(r)} = D_{l+1}^{(2)}, \\ 12 & \text{if } X_N^{(r)} = E_6^{(2)}, \\ 6 & \text{if } X_N^{(r)} = D_4^{(3)}. \end{cases} \tag{51}$$

Remark 11. $X_N^{(r)} = A_{2l-1}^{(2)}, D_{l+1}^{(2)}, E_6^{(2)}, D_4^{(3)}$ の全ての場合に, 各 $k \in \mathbb{Z}/r\mathbb{Z}$ に対して

$$\dim_{\mathbb{C}} \mathfrak{g}_k = (1+h^\vee) \dim_{\mathbb{C}} \mathfrak{h}_k \tag{52}$$

である事が直接計算により確かめられる. 以下では, $l_k := \dim_{\mathbb{C}} \mathfrak{h}_k$ と書く事にする. この時 $l_0 = l$, $l_k = l_{-k}$ である.

4.2. B_l, C_l, F_4, G_2 型の場合の結果. 以下, $X_N^{(r)} = A_{2l-1}^{(2)}, D_{l+1}^{(2)}, E_6^{(2)}, D_4^{(3)}$ とする. $X_N^{(r)}$ 型の twisted affine Lie 環 $\hat{\mathfrak{g}} = \mathfrak{g}(X_N^{(r)})$ についても nontwisted affine Lie 環の時と同様に, 既約 highest weight 表現や basic 表現等が考えられる. 即ち, $\Lambda_0 \in (\hat{\mathfrak{h}})^*$ は $\Lambda_0(\mathfrak{h}_{\bar{0}}) = 0$, $\Lambda_0(c) = 1$, $\Lambda_0(d) = 0$ により定まる basic fundamental weight とし, $V := \hat{L}(\Lambda_0)$ は Λ_0 を highest weight とする $\hat{\mathfrak{g}}$ の既約 highest weight 表現 (basic 表現) とする. この basic 表現 V に $d \in \hat{\mathfrak{g}}$ を用いて $\mathbb{Z}$-次数付け (basic gradation):

$$V = \bigoplus_{m \in \mathbb{Z}_{\ge 0}} V_m, \quad V_m := \{v \in V \mid dv = -mv\} \tag{53}$$

を行った時の $\dim_{\mathbb{C}} V_m$ の母関数 (graded dimension)

$$f(q) := \dim_q V = \sum_{m \ge 0} (\dim_{\mathbb{C}} V_m)\, q^m \tag{54}$$

に関して, Fact 1 と同様の次の結果が知られている ([K4] 参照).

Fact 3. $\hat{\mathfrak{g}} = \mathfrak{g}(X_N^{(r)})$ を $X_N^{(r)}$ 型の *twisted affine Lie* 環 とする. この時, $\hat{\mathfrak{g}}$ の *basic* 表現 $V = \oplus_{m \ge 0} V_m$ の *graded dimension* $f(q) = \dim_q V$ は, 次の様に表せる.

$$f(q) = \left(\prod_{k \in \mathbb{Z}/r\mathbb{Z}} \phi_k(q)^{-l_k} \right) \cdot \Theta_Q(q). \tag{55}$$

ここで, $Q \subset (\mathfrak{h}_{\bar{0}})^* \hookrightarrow (\hat{\mathfrak{h}})^*$ は Y_L 型の有限次元複素単純 *Lie* 環 $\mathfrak{g}_{\bar{0}} = \mathfrak{g}(Y_L)$ の *root lattice* で,

$$\Theta_Q(q) := \sum_{\alpha \in Q} q^{\frac{1}{2}(\alpha|\alpha)^\wedge} = \sum_{\alpha \in Q} q^{\frac{r}{2}(\alpha|\alpha)} \tag{56}$$

である. 又, 各 $k \in \mathbb{Z}/r\mathbb{Z}$ に対して

$$\phi_k(q) := \prod_{\substack{n \geq 1 \\ n = k}} (1 - q^n) \tag{57}$$

である.

Remark 12. (47) 式にある様に, $h_1, h_2 \in \mathfrak{h}_{\bar{0}} \subset \hat{\mathfrak{g}} \cap \mathfrak{g}$ に対して $(h_1|h_2)^\wedge = r^{-1}(h_1|h_2)$ であったから, $\alpha, \beta \in (\mathfrak{h}_{\bar{0}})^* \subset (\hat{\mathfrak{h}})^* \cap \mathfrak{h}^*$ に対して

$$(\alpha|\beta)^\wedge = r(\alpha|\beta) = r\langle \alpha, \beta \rangle \tag{58}$$

が成り立つ.

さらに, basic 表現 $V = \oplus_{m \geq 0} V_m$ の各斉次成分 V_m は $\mathfrak{g}_{\bar{0}}$ の作用で不変 ($\mathfrak{g}_{\bar{0}} V_m \subset V_m$) であり, 従って V_m は $\mathfrak{g}_{\bar{0}}$ の表現として

$$V_m = \bigoplus_{\lambda \in P_+} \Phi(\Lambda_0, \lambda)_m \, L(\lambda) \tag{59}$$

と既約分解する. ここで $P_+ := \{\lambda \in (\mathfrak{h}_{\bar{0}})^* \mid \frac{2(\lambda|\alpha_i)}{(\alpha_i|\alpha_i)} \in \mathbb{Z}_{\geq 0},\ 1 \leq i \leq l\}$ は $\mathfrak{g}_{\bar{0}} = \mathfrak{g}(Y_L)$ の dominant integral weight の全体, $L(\lambda)$ は $\lambda \in P_+$ を highest weight とする $\mathfrak{g}_{\bar{0}} = \mathfrak{g}(Y_L)$ の有限次元既約 highest weight 表現である. この重複度 $\Phi(\Lambda_0, \lambda)_m$ の母関数

$$\Phi(\Lambda_0, \lambda)(q) := \sum_{m \geq 0} \Phi(\Lambda_0, \lambda)_m \, q^m \tag{60}$$

に関して, Fact 2 と同様の次の結果が知られている ([K4] 参照).

Fact 4. $\hat{\mathfrak{g}} = \mathfrak{g}(X_N^{(r)})$ を $X_N^{(r)}$ 型の *twisted affine Lie* 環, $\lambda \in P_+$ とする. この時, 重複度 $\Phi(\Lambda_0, \lambda)_m$ の母関数 $\Phi(\Lambda_0, \lambda)(q)$ は, $\lambda \notin Q$ に対しては $\Phi(\Lambda_0, \lambda)(q) = 0$ で, そして $\lambda \in Q$ に対しては

$$\Phi(\Lambda_0, \lambda)(q) = \left(\prod_{k \in \mathbb{Z}/r\mathbb{Z}} \phi_k(q)^{-l_k} \right) \cdot q^{\frac{r}{2}(\lambda|\lambda)} \prod_{\alpha \in (\Delta_0)_+} \left(1 - q^{r(\lambda+\rho|\alpha)}\right) \tag{61}$$

で与えられる. ここで $\rho = \frac{1}{2} \sum_{\alpha \in (\Delta_0)_+} \alpha$ である.

上記の Fact 3, 4 から, Proposition 1 と同様にして次が示せる.

Proposition 2. Q を B_l, C_l, F_4, G_2 型の有限次元複素単純 *Lie* 環 $\mathfrak{g}_{\bar{0}} = \mathfrak{g}(Y_L)$ の *root lattice*, $(\cdot|\cdot)$ を $(\mathfrak{h}_{\bar{0}})^*$ 上の *normalized* (全ての *long root* $\alpha \in (\Delta_{\bar{0}})_l$ に対して $(\alpha|\alpha) = 2$ である) *Killing form* とする. この時, $\Theta_Q(q) = \sum_{\alpha \in Q} q^{\frac{r}{2}(\alpha|\alpha)}$ に関して次の等式が成り立つ.

$$\Theta_Q(q) = \sum_{\lambda \in P_+ \cap Q} d(\lambda)\, q^{\frac{r}{2}(\lambda|\lambda)} \prod_{\alpha \in (\Delta_{\bar{0}})_+} \left(1 - q^{r(\lambda+\rho|\alpha)}\right). \tag{62}$$

但し *dominant integral weight* $\lambda \in P_+ \subset (\mathfrak{h}_{\bar{0}})^*$ に対して, $d(\lambda)$ は λ を *highest weight* とする $\mathfrak{g}_{\bar{0}}$ の有限次元既約 *highest weight* 表現 $L(\lambda)$ の次元 $\dim_{\mathbb{C}} L(\lambda)$ を表し,

$$d(\lambda) = \prod_{\alpha \in (\Delta_{\bar{0}})_+} \frac{(\lambda + \rho|\alpha)}{(\rho|\alpha)} \tag{63}$$

で与えられる.

Remark 13. Proposition 2 の (62) 式において q^r をあらためて q と置けば, Proposition 1 の (13) 式と同じ形の式となる.

以下では, Theorem 1 と同様の結果が B_l, C_l, F_4, G_2 型の有限次元複素単純 Lie 環 $\mathfrak{g}_{\bar{0}} = \mathfrak{g}(Y_L)$ の root lattice Q に対しても成り立つ事を説明する. 先ず, 各 $k \in \mathbb{Z}/r\mathbb{Z}$ に対して

$$h_k(q) := \phi_k(q)^{-l_k}, \quad H_k(q) := \log(h_k(q)) \tag{64}$$

とする. この時 Lemma 2, Lemma 3 のそれぞれと同様にして, 次の 2 つの補題を得る.

Lemma 4. 各 $k \in \mathbb{Z}/r\mathbb{Z}$ に対して,

$$q\frac{d}{dq}H_k(q) = l_k \sum_{\substack{n \geq 1 \\ n \equiv k}} n \sum_{j \geq 1} q^{nj} \tag{65}$$

が成り立つ.

Lemma 5. 各 $k \in \mathbb{Z}/r\mathbb{Z}$ に対して,

$$\frac{d}{dq}h_k(q) = h_k(q) \cdot \frac{d}{dq}H_k(q) \tag{66}$$

が成り立つ.

次がこの §4 の主定理である.

Theorem 2. Q を B_l, C_l, F_4, G_2 型の有限次元複素単純 *Lie* 環 $\mathfrak{g}_{\bar{0}} = \mathfrak{g}(Y_L)$ の *root lattice*, $(\cdot|\cdot)$ を *Cartan subalgebra* の *dual* $(\mathfrak{h}_{\bar{0}})^*$ 上の *normalized* (全ての *long root* $\alpha \in (\Delta_{\bar{0}})_l$ に対して $(\alpha|\alpha) = 2$ である) *Killing form* とする. この時, $\Theta_Q(q) = \sum_{\alpha \in Q} q^{\frac{r}{2}(\alpha|\alpha)}$ に関して次の等式が成り立つ.

$$2r^{-1}(1+h^\vee)\, q\frac{d}{dq}\Theta_Q(q) = \sum_{\lambda \in P_+ \cap Q} d(\lambda)(\lambda+\rho|\lambda)\, q^{\frac{r}{2}(\lambda|\lambda)} \prod_{\alpha \in (\Delta_{\bar{0}})_+} \left(1 - q^{r(\lambda+\rho|\alpha)}\right). \tag{67}$$

但し, $h^\vee$ は (42), (51) 式で与えられる *dual Coxeter number* であり, $\rho = \frac{1}{2}\sum_{\alpha \in \Delta_{\bar{0}}} \alpha$, $d(\lambda) = \dim_{\mathbb{C}} L(\lambda)$ である.

Remark 14. Theorem 2 の (67) 式において q^r をあらためて q と置けば, Theorem 1 の (28) 式と同じ形の式となる.

(Theorem 2 の証明.) 有限次元複素単純 Lie 環 $\mathfrak{g}_{\bar{0}} = \mathfrak{g}(Y_L)$ の Casimir operator Ω について, $\mathrm{Tr}(\Omega|_{V_m}) \in \mathbb{C}$ の母関数

$$g(q) := \sum_{m \geq 0} \mathrm{Tr}(\Omega|_{V_m})\, q^m$$

を二通りの方法で計算する. twisted affine Lie 環 $\hat{\mathfrak{g}}$ の Casimir operator $\hat{\Omega}$ は, basic 表現 $V = \hat{L}(\Lambda_0)$ 上に scalar $(\Lambda_0 + 2\hat{\rho}|\Lambda_0)^\wedge$ として作用する. ここで $\hat{\rho} \in (\hat{\mathfrak{h}})^*$ は, $2(\rho|\alpha_i)^\wedge = (\alpha_i|\alpha_i)^\wedge$, $0 \leq i \leq l$, と $(\hat{\rho}|\Lambda_0)^\wedge = 0$ により一意的に定まる元である. ところが $(\Lambda_0|\Lambda_0)^\wedge = 0$ であるから, 結局 $\hat{\Omega}$ は V 上に zero operator として作用している事になる. 一方, $\hat{\Omega}$ の表示 (49) 式と $\Lambda_0(c) = 1$ である事から, V の各斉次成分 V_m 上の作用素として

$$0 = r\Omega|_{V_m} - 2(1+h^\vee)\, m\, I_{V_m} + 2r \sum_{k \in \mathbb{Z}/r\mathbb{Z}} \sum_{\substack{n \geq 1 \\ \bar{n}=k}} \sum_{i=1}^{\dim \mathfrak{g}_k} u^{(k)i}(-n) u_i^{(k)}(n)|_{V_m}$$

が成り立つ事が分かる. よって結局, 各 $m \geq 0$ に対して

$$r\mathrm{Tr}(\Omega|_{V_m}) = 2(1+h^\vee)\, m\, (\dim_{\mathbb{C}} V_m) - 2r \sum_{k \in \mathbb{Z}/r\mathbb{Z}} \sum_{\substack{n \geq 1 \\ \bar{n}=k}} \mathrm{Tr}\left(\left(\sum_{i=1}^{\dim \mathfrak{g}_k} u^{(k)i}(-n) u_i^{(k)}(n) \right)|_{V_m} \right) \tag{68}$$

である.

Claim 2. 各 $k \in \mathbb{Z}/r\mathbb{Z}$ と $\bar{n} = k$ なる整数 $n \geq 1$ に対して

$$\mathrm{Tr}\left(\left(\sum_{i=1}^{\dim \mathfrak{g}_k} u^{(k)i}(-n) u_i^{(k)}(n) \right)\Big|_{V_m} \right) = r^{-1} (\dim_{\mathbb{C}} \mathfrak{g}_k)\, n \sum_{j \geq 1} \dim_{\mathbb{C}} V_{m-nj} \tag{69}$$

が成り立つ.

今, この Claim 2 を認める事にすれば, (68), (69) の両式を合わせる事により

$$r\mathrm{Tr}(\Omega|_{V_m}) = 2(1+h^\vee)\, m (\dim_{\mathbb{C}} V_m) - 2 \sum_{k \in \mathbb{Z}/r\mathbb{Z}} (\dim_{\mathbb{C}} \mathfrak{g}_k) \sum_{\substack{n \geq 1 \\ \bar{n} = k}} n \sum_{j \geq 1} \dim_{\mathbb{C}} V_{m-nj}$$

となる. 従って, Theorem 1 の証明と同様にして

$$\begin{aligned} g(q) &= \sum_{m \geq 0} \mathrm{Tr}(\Omega|_{V_m})\, q^m \\ &= 2r^{-1}(1+h^\vee)\, q \frac{d}{dq} f(q) - 2r^{-1} \sum_{k \in \mathbb{Z}/r\mathbb{Z}} (\dim_{\mathbb{C}} \mathfrak{g}_k) \cdot l_k^{-1} f(q) \cdot q \frac{d}{dq} H_k(q) && \text{“by (65)”} \\ &= 2r^{-1}(1+h^\vee)\, q \left\{ \frac{d}{dq} f(q) - f(q) \cdot \sum_{k \in \mathbb{Z}/r\mathbb{Z}} \frac{d}{dq} H_k(q) \right\} && \text{“by (52)”} \\ &= 2r^{-1}(1+h^\vee)\, q \left(\prod_{k \in \mathbb{Z}/r\mathbb{Z}} h_k(q) \right) \cdot \frac{d}{dq} \Theta_Q(q) && \text{“by (66)”} \end{aligned}$$

と表せる事が分かる.

一方 Fact 4 から, やはり Theorem 1 の証明と同様にして

$$g(q) = \left(\prod_{k \in \mathbb{Z}/r\mathbb{Z}} h_k(q) \right) \cdot \sum_{\lambda \in P_+ \cap Q} d(\lambda)(\lambda + 2\rho|\lambda)\, q^{\frac{r}{2}(\lambda|\lambda)} \prod_{\alpha \in (\Delta_0)_+} \left(1 - q^{r(\lambda+\rho|\alpha)}\right)$$

が示せる. そこで, これら二通りの $g(q)$ の表示を比べる事により, Theorem 2 の等式が得られる. □

(Claim 2 の証明.) 先ず, 各 $k \in \mathbb{Z}/r\mathbb{Z}$, $\bar{n} = k$ なる整数 $n \geq 1$, $1 \leq i \leq \dim_{\mathbb{C}} \mathfrak{g}_k$ に対して, 交換関係 (2) から ($c' = r^{-1}c$ である事に注意して)

$$\begin{aligned} [t^n \otimes u_i^{(k)}, t^{-n} \otimes u^{(k)i}] &= t^0 \otimes [u_i^{(k)}, u^{(k)i}] + n (u_i^{(k)} | u^{(k)i}) c' \\ &= [u_i^{(k)}, u^{(k)i}] + r^{-1} nc \end{aligned}$$

である. よって (50) 式より, 各 $k \in \mathbb{Z}/r\mathbb{Z}$ と $\bar{n} = k$ なる整数 $n \geq 1$ に対して,

$$\sum_{i=1}^{\dim \mathfrak{g}_k} [t^n \otimes u_i^{(k)}, t^{-n} \otimes u^{(k)i}] = r^{-1}(\dim_{\mathbb{C}} \mathfrak{g}_k)\, nc \tag{70}$$

を得る. 後は Claim 1 の証明と同様にして,

$$\mathrm{Tr}\left((\sum_{i=1}^{\dim \mathfrak{g}_k} u^{(k)i}(-n) u_i^{(k)}(n))|_{V_m} \right) = r^{-1}(\dim_{\mathbb{C}} \mathfrak{g}_k)\, n \sum_{j \geq 1} \dim_{\mathbb{C}} V_{m-nj}$$

である事が示せる. □

REFERENCES

[FK] I. B. Frenkel and V. G. Kac, *Basic representations of affine Lie algebras and dual resonance models*, Invent. Math. 62 (1980), 23–66.

[K1] V. G. Kac, *Infinite-dimensional algebras, Dedekind's η-function, classical Möbius function and the very strange formula*, Adv. Math. 30 (1978), 85–136.

[K2] ———, *An elucidation of "Infinite-dimensional algebras ... and the very strange formula." $E_8^{(1)}$ and the cube root of the modular invariant j*, Adv. Math. 35 (1980), 264–273.

[K3] ———, *A remark on the Conway-Norton conjecture about the "Monster" simple group*, Proc. Natl. Acad. Sci. U.S.A. 77 (1980), 5048–5049.

[K4] ———, *Infinite Dimensional Lie Algebras* (3rd ed.), Cambridge Univ. Press, Cambridge, 1990.

[KP] V. G. Kac and D. H. Peterson, *Infinite-dimensional Lie algebras, theta functions and modular forms*, Adv. Math. 53 (1984), 125–264.

[KT] V. G. Kac and I. T. Todorov, *Affine orbifolds and rational conformal field theory extensions of $W_{1+\infty}$*, Commun. Math. Phys. 190 (1997), 57–111.

[KW] V. G. Kac and M. Wakimoto, *Modular and conformal invariance constraints in representation theory of affine algebras*, Adv. Math. 70 (1988), 156–236.

[W] Z.-X. Wan, *Introduction to Kac-Moody Algebra*, World Scientific, Singapore, 1991.

〒305−8571 つくば市天王台 1−1−1

E-mail address: naito@math.tsukuba.ac.jp

多重ゼータ値間の或る関係式の集合について

大野泰生

大阪大学 理学研究科・学振研究員

Riemann の $\zeta(n)$ の多重化の一種である多重ゼータ値の研究は、Euler までさかのぼることができて、最近では D. Zagier や M. Hoffman, J. Borwein 達によって盛んに行われています。多重ゼータ値を調べることは、ガロア表現、mixed Tate motives や Vassiliev-Kontsevich knot invarians などの研究と関係していると言われ、整数論以外の分野からも広く興味を持たれているようです。

本稿では、多重ゼータ値間の関係式を与えている "sum formula" と "duality formula" を含む、合計三つの既知の定理（定理１、２、３）を、同時に一般化した定理（定理４）について述べたいと思います。

第１節では Riemann ゼータ関数と多重ゼータ値について、定義も含めて復習します。第２節では、"sum formula" と "duality formula" を含めた、多重ゼータ値について知られている関係式の系列を３つ復習します。第３節では、今回の主結果を説明します。第４節では、Drinfel'd, Goncharov, Kontsevich, Zagier が与えた予想において期待されている関係式の個数と、主結果から得られる関係式の個数を比較します。第５節では、荒川一金子 [1] によって導入された、多重ベルヌーイ数を非正整数点での値に持つゼータ関数の、正整数点の値に対して、主結果を用いた考察を行います。

1 Riemann のゼータ関数と多重ゼータ値

Riemann のゼータ関数 $\zeta(s)$ は、

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

で定義される、整数論における重要な関数のひとつです。この関数は、$Re(s) > 1$ の範囲で収束し、$s = 1$ の一位の極を除く全 s–平面で、正則に解析接続されます。Riemann のゼータ関数については、まだまだわからないことも多いようで、有名な未解決問題として

は、 Riemann 予想などがあります。本稿で扱っている整数点での値（特殊値）に関しても、負の整数点と正の偶数点での値がベルヌーイ数と π を使って書けること（負の偶数点での値がすべて 0 であること）が判っているのですが、$\zeta(3)$ や $\zeta(5)$ をはじめとして、正の奇数点での具体的な値はわかっていないようです。

Euler は、Riemann のゼータ関数を、２変数に拡張した級数の、整数点での値について研究していたようです。それは、

$$\zeta(k_1,k_2)=\sum_{0<m_1<m_2}\frac{1}{{m_1}^{k_1}{m_2}^{k_2}}$$

というもので、この右辺は、$k_1\geq 1$ かつ $k_2>1$ で収束します。 Euler はこの級数と Riemann のゼータ関数の特殊値の関係を研究し、

$$\zeta(1,k-1)=\frac{k-1}{2}\zeta(k)-\frac{1}{2}\sum_{r=2}^{k-2}\zeta(r)\zeta(k-r)\qquad\text{(Proved by Euler.)}$$

といった結果を残しています。この関係式で $k=3$ とおくと、

$$\zeta(1,2)=\zeta(3)\quad\text{つまり、}\quad\sum_{0<m_1<m_2}\frac{1}{m_1{m_2}^2}=\sum_{0<m}\frac{1}{m^3}$$

という、おそらく多重ゼータ値の最も古い関係式が得られます。

この、$\zeta(1,2)=\zeta(3)$ は、例えば以下のように示せます。

$$\begin{aligned}\zeta(3)+\zeta(1,2)&=\sum_{n_1\geq 1}\frac{1}{{n_1}^2}\sum_{j=1}^{n_1}\frac{1}{j}\\&=\sum_{n_1\geq 1}\frac{1}{{n_1}^2}\sum_{n_2\geq 1}\Big(\frac{1}{n_2}-\frac{1}{n_1+n_2}\Big)\\&=\sum_{n_1\geq 1,\ n_2\geq 1}\frac{1}{n_1(n_1+n_2)^2}+\sum_{n_1\geq 1,\ n_2\geq 1}\frac{1}{n_2(n_1+n_2)^2}\\&=2\sum_{0<m_1<m_2}\frac{1}{m_1{m_2}^2}\ =\ 2\zeta(1,2).\end{aligned}$$

上の Euler の関係式に $k=4,\ 5$ を代入すると、

$$\zeta(1,3)=\frac{3}{2}\zeta(4)-\frac{1}{2}\zeta(2)^2$$

$$\zeta(1,4)=2\zeta(5)-\zeta(2)\zeta(3)$$

などの関係式が得られます。このように、ここに登場する特殊値の間には、いろいろな関係式が存在することが判っています。

上の関係式では、"2重ゼータ値" が $\zeta(1,k-1)$ の形だけになりますから、ここで $\zeta(2,2)$ を考えてみることにします。

$$\begin{aligned}
\zeta(2)^2 &= \Big(\sum_{m_1=1}^{\infty}\frac{1}{{m_1}^2}\Big)\Big(\sum_{m_2=1}^{\infty}\frac{1}{{m_2}^2}\Big)\\
&= \sum_{m_1=1}^{\infty}\sum_{m_2=1}^{\infty}\frac{1}{{m_1}^2{m_2}^2}\\
&= \Big(\sum_{0<m_1<m_2}\frac{1}{{m_1}^2{m_2}^2}\Big)+\Big(\sum_{0<m_1=m_2}\frac{1}{{m_1}^2{m_2}^2}\Big)+\Big(\sum_{0<m_2<m_1}\frac{1}{{m_1}^2{m_2}^2}\Big)\\
&= 2\Big(\sum_{0<m_1<m_2}\frac{1}{{m_1}^2{m_2}^2}\Big)+\Big(\sum_{0<m}\frac{1}{m^4}\Big)\\
&= 2\zeta(2,2)+\zeta(4)
\end{aligned}$$

従って、

$$\zeta(2,2)=\frac{1}{2}(\zeta(2)^2-\zeta(4))$$

という関係式が得られるのです。

この関係式と先の $\zeta(1,3)$ の式とを合わせると、

$$\zeta(1,3)+\zeta(2,2)=\zeta(4)$$

という関係式も得られます。この関係式は、後に2節で紹介する "sum formula" と呼ばれる関係式の一例になっています。

同様に $\zeta(2)$ と $\zeta(3)$ の積を計算すると、

$$\zeta(2)\zeta(3)=\zeta(2,3)+\zeta(5)+\zeta(3,2)$$

という関係式が得られ、これと先の $\zeta(1,4)$ の式とを組み合わせると、

$$\zeta(1,4)+\zeta(2,3)+\zeta(3,2)=\zeta(5)$$

という関係式が得られます。この関係式も "sum formula" の一例です。

Euler の2重化の方向に従って更に多重化を進めると、以下のように級数（多重ゼータ値）が定義されます。

整数 $n \geq 1$, $k_1, k_2, \ldots, k_{n-1} \geq 1$ および $k_n \geq 2$ に対して、

$$\mathrm{k} = (k_1, k_2, \ldots, k_n)$$

を index set と呼ぶことにし、これに対する多重ゼータ値 $\zeta(\mathrm{k})$ を、

$$\zeta(\mathrm{k}) = \zeta(k_1, k_2, \ldots, k_n) = \sum_{0<m_1<m_2<\cdots<m_n} \frac{1}{{m_1}^{k_1} {m_2}^{k_2} \cdots {m_n}^{k_n}}$$

で定義します。ここで、$k = k_1 + k_2 + \cdots + k_n$ を k の total weight と言い、n を k の depth と言います。従って、Euler が研究していたのは、depth が 2 の場合ということになります。

多重ゼータ値の満たす関係式が多く存在しそうなことは以前から想像されていたようですが、具体的な関係式を求める研究は、さほど盛んに行われていたわけではないようです。ところが近年になって、depth $n \geq 1$ の多重ゼータ値の満たす関係式を調べることが、mixed Tate motives や knot invariants など様々な分野の研究と関係していることが徐々に判ってきて、D. Zagier, M. Hoffman, J. Borwein, A. Granville など多くの数学者や、 D. J. Broadhurst 達物理系の研究者によって盛んな研究が行われています。

2　既知の関係式の３つの系列

以下では、関係式を系統立てて与えている既知の定理のうちの３つを復習します。第３節で述べる主結果は、これら３つの定理を同時に包含し、拡張したものになっています。

最初は 1992年に与えられた、depth n と depth $n+1$ の多重ゼータ値の間の関係式です。

定理 1 (Hoffman[7]) 任意の *index set* $\mathrm{k} = (k_1, k_2, \ldots, k_n)$ に対して以下が成り立つ。

$$\sum_{\substack{a_1+a_2+\cdots+a_n=1 \\ \forall a_j \geq 0}} \zeta(a_1 + k_1, a_2 + k_2, \ldots, a_n + k_n)$$

$$= \sum_{\substack{1 \leq l \leq n \\ k_l \geq 2}} \sum_{j=0}^{k_l - 2} \zeta(k_1, \ldots, k_{l-1}, j+1, k_l - j, k_{l+1}, \ldots, k_n).$$

次に "duality formula" を述べるために dual index を定義します。任意の index set k に対して、

$$\mathsf{k}=(\underbrace{1,\ldots,1}_{a_1-1},b_1+1,\underbrace{1,\ldots,1}_{a_2-1},b_2+1,\ldots,\underbrace{1,\ldots,1}_{a_s-1},b_s+1)$$

をみたす整数 $s\geq 1$ と $a_1,b_1,a_2,b_2,\ldots,a_s,b_s\geq 1$ は、一意的に決まりますが、それらに対して index set k' を

$$\mathsf{k}'=(\underbrace{1,\ldots,1}_{b_s-1},a_s+1,\underbrace{1,\ldots,1}_{b_{s-1}-1},a_{s-1}+1,\ldots,\underbrace{1,\ldots,1}_{b_1-1},a_1+1)$$

と定めるとき、k' を k の dual index set と呼ぶことにします。

"duality formula" とは以下のような定理です。

定理 2 (duality formula cf. [2][18]) 任意の *index set* k とその *dual index set* k' に対して以下が成り立つ。

$$\zeta(\mathsf{k}')=\zeta(\mathsf{k}).$$

次に、 "sum formula"とは以下のように、多重ゼータ値の和を Riemann のゼータ関数の特殊値で表した美しい定理です。

定理 3 (sum formula cf. [2][7]) 整数 $0<n<k$ に対して以下が成り立つ。

$$\sum_{\substack{k_1,k_2,\ldots,k_{n-1}\geq 1,k_n\geq 2,\\ k_1+k_2+\cdots+k_n=k}}\zeta(k_1,k_2,\ldots,k_n)=\zeta(k).$$

定理2と定理3の証明には、Kontsevich によって与えられた、多重ゼータ値の " Drinfel'd 積分表示" (cf.[18]) と呼ばれる以下の表記が用いられます。

$$\zeta(k_1,\ldots,k_n)=I(1,\underbrace{0,\ldots,0}_{k_1-1},1,\underbrace{0,\ldots,0}_{k_2-1},\ldots,1,\underbrace{0,\ldots,0}_{k_n-1}),$$

ただしここで $\varepsilon_1=1,\varepsilon_k=0,\varepsilon_2,\ldots,\varepsilon_{k-1}\in\{0,1\}$ とし、$A_0(t)=t$, $A_1(t)=1-t$ とするとき、

$$I(\varepsilon_1,\ldots,\varepsilon_k)=\int\cdots\int_{0<t_1<\cdots<t_k<1}\frac{dt_1}{A_{\varepsilon_1}(t_1)}\cdots\frac{dt_k}{A_{\varepsilon_k}(t_k)}$$

とします。

3　主結果

今回、第2節で復習した3つの定理の拡張が、以下のように得られました。どういう形で、第2節の3つの定理が含まれているかについては、主定理の後の注意で確認することにします。

定理 4 (主結果) 任意の *index set* $\mathsf{k}=(k_1,k_2,\ldots,k_n)$ と整数 $l\geq 0$ に対して $Z(\mathsf{k};l)$ を

$$Z(\mathsf{k};l)=\sum_{\substack{c_1+c_2+\cdots+c_n=l\\ \forall c_j\geq 0}}\zeta(k_1+c_1,k_2+c_2,\ldots,k_n+c_n),$$

とし、k' を k の *dual index set* とする。この時、次が成り立つ。

$$Z(\mathsf{k}';l)=Z(\mathsf{k};l).$$

注意　上の定理4を $l=0$ に制限すれば、主張が先の定理2 (duality formula) と同じになることが容易にわかります。

また、定理4で、k のdepth を 1 に制限すれば、これは定理3 (sum formula) と同じ主張になります。実際、$0<n<k$ に対して、

$$\mathsf{k}=(n+1)$$

の dual index set は

$$\mathsf{k}'=(\underbrace{1,1,\ldots,1}_{n-1},2)$$

ですから、

$$Z(\mathsf{k}';k-n-1)=\sum_{\substack{c_1+c_2+\cdots+c_n=k-n-1\\ \forall c_j\geq 0}}\zeta(1+c_1,1+c_2,\ldots,1+c_{n-1},2+c_n),$$

となり、この右辺は結局 total weight k でdepth n の多重ゼータ値全部の和になります。一方、定理の右辺は $Z(\mathsf{k};k-n-1)=\zeta(k)$ です。

さらに、定理4は $l=1$ の場合に定理1も含んでいます。つまり定理1の右辺の多重ゼータ値たちをすべて定理2で書き換えると、定理4で $l=1$ とした場合と全く同じ主張になります。

4 Drinfel'd, Goncharov, Kontsevich, Zagier の予想との比較

total weight が k の多重ゼータ値たちの Q-係数の一次結合全体のなすベクトル空間を $\mathbf{A}_k$ とする時、

$$\sum_{k=2}^{\infty} \mathbf{A}_k$$

の環構造を理解することが、いくつかの分野の研究とつながって大問題となっているようですが、この問題に関連して、各 $\mathbf{A}_k$ たちの Q 上の次元について以下の予想が知られています。

予想 1 (Drinfel'd, Goncharov, Kontsevich, Zagier cf. [2],[18]) 数列 d_k を

$$d_2 = d_3 = d_4 = 1, \quad d_k = d_{k-2} + d_{k-3}$$

で定義する時、

$$dim_{\mathbf{Q}} \mathbf{A}_k \stackrel{?}{=} d_k.$$

今回の定理 4 から得られる独立な関係式の個数と、上の予想で必要とされている独立な関係式の個数とを比較すると次頁の表のようになります。従って、この定理の範疇に入っていない独立な関係式が、例えば weight $k = 10$ では 50 個、weight $k = 11$ では 92 個存在すると予想されていることになります。逆に言うと、$dim_{\mathbf{Q}} \mathbf{A}_{10} \leq 57$, $dim_{\mathbf{Q}} \mathbf{A}_{11} \leq 101$ が定理 4 から導かれることになります。weight $4 < k \leq 11$ の範囲では、予想される独立な関係式の個数の 7 割以上が定理 4 から得られることがわかります。

予想 1 と定理 4 の比較

total weight	2	3	4	5	6	7	8	9	10	11
多重ゼータ値の個数 (index set の個数)	1	2	4	8	16	32	64	128	256	512
self-dual な index set の個数	1	0	2	0	4	0	8	0	16	0
duality の個数	0	1	1	4	6	16	28	64	120	256
duality の個数の累計	0	1	2	6	12	28	56	120	240	496
定理 4 で得られる独立な関係式の個数	0	1	2	5	10	23	46	98	199	411
予想されている独立な関係式の個数	0	1	3	6	14	29	60	123	249	503
予想されている次元	1	1	1	2	2	3	4	5	7	9

(定理 4 で得られる独立な関係式の個数の算出は最初に金子先生によって行われました。)

5　荒川-金子のゼータ関数の特殊値への応用

多重ベルヌーイ数 $B_n^{(k)}$ は、通常のベルヌーイ数の一般化として金子[10] により定義されました（ここでは [2] の定義に従います)。

$$\frac{Li_k(1-e^{-x})}{e^x-1}=\sum_{n=0}^{\infty}B_n^{(k)}\frac{x^n}{n!},$$

ここで、任意の整数 k に対し、$Li_k(z)=\sum_{m=0}^{\infty}\frac{z^m}{m^k}$ （$k\geq 1$ の時 k-th polylogarithm と呼ばれている関数）です。$k=1$ の時 $B_n^{(1)}$ は通常のベルヌーイ数です。

昨年 荒川一金子[1] によって、$k\geq 1$ に対して以下の関数 $\xi_k(s)$ が定義されました。

$$\xi_k(s)=\frac{1}{\Gamma(s)}\int_0^{\infty}\frac{t^{s-1}}{e^t-1}Li_k(1-e^{-t})dt.$$

荒川一金子 はこの関数が $Re(s)>0$ で収束することを示し、特に$k=1$ の時に $\xi_1(s)=s\zeta(s+1)$ であることを示しました。また $\xi_k(s)$ と多重ベルヌーイ数との関係を以下の形で与えました。

定理 5 (荒川一金子 [1][2]) 関数 $\xi_k(s)$ は s の整関数に解析接続され、非正整数点での特殊値は以下で与えられる。

$$\xi_k(-m)=(-1)^m B_m^{(k)} \qquad (m=0,1,2,\ldots).$$

そして、このゼータ関数の正整数点での値については以下の定理が与えられました。

定理 6 (荒川一金子 [1][2]) (i) 整数 $k\geq 1$ と $m\geq 0$に対して

$$\xi_k(m+1)=\sum_{\substack{a_1+a_2+\cdots+a_k=m\\ \forall a_j\geq 0}}(a_k+1)\zeta(a_1+1,a_2+1,\ldots,a_{k-1}+1,a_k+2).$$

(ii) 偶数 $k\geq 2$ に対して

$$\xi_k(2)=\frac{1}{2}\sum_{i=0}^{k-2}(-1)^i\zeta(i+2)\zeta(k-i).$$

この定理6の (i) に定理4を使うと、$\xi_k(s)$ の正整数点での値は以下のように書き換えることができます。

定理 7 整数 $k \geq 1$ と $n \geq 1$ に対して

$$\xi_k(n) = \sum_{0<m_1 \leq m_2 \leq \cdots \leq m_n} \frac{1}{m_1 m_2 \cdots m_{n-1} {m_n}^{k+1}}.$$

この表記を用いると、例えば荒川一金子のゼータ関数の $s=2$ での値が、

$$\begin{aligned} \xi_k(2) &= \zeta(1,k+1) + \zeta(k+2) \\ &= \frac{k+3}{2}\zeta(k+2) - \frac{1}{2}\sum_{r=2}^{k}\zeta(r)\zeta(k-r+2). \end{aligned}$$

と書き換えられて、k の偶奇によらずに Riemann のゼータ関数で書けるという事実が、以前より見えやすくなります。(ここで、$\zeta(1,k+1)$ の書き換えには、第 1 節の最初に述べた Euler の結果を用いています。)

参考文献

[1] T. Arakawa and M. Kaneko, Multiple zeta values, poly-Bernoulli numbers, and related zeta functions, *preprint (to appear in Nagoya Math. J.)*.

[2] 荒川恒男 金子昌信, 多重ゼータ値、多重ベルヌーイ数 および関連するゼータ関数, 津田塾大学数学・計算機科学研究所報, 13, 第 2 回津田塾大学整数論シンポジウム報告集 (1996), 133-144.

[3] J. M. Borwein, D. M. Bradley and D. J. Broadhurst, Evaluations of k-fold Euler/Zagier sums: a compendium of results for arbitrary k, *preprint* (1996).

[4] D. Borwein, J. M. Borwein and R. Girgensohn, Explicit evaluation of Euler sums, *Proc. Edin. Math. Soc.*, **38** (1995), 277-294.

[5] D. J. Broadhurst, A proof of Zagier's conjecture, *preprint* (1997).

[6] D. J. Broadhurst, Generalization of Zagier's observation, *preprint* (1997).

[7] M. Hoffman, Multiple harmonic series, *Pacific J. Math.*, **152** (1992), 275-290.

[8] J. G. Huard, K. S. Williams and Zhang Nan-Yue, On Tornheim's double series, *Acta Arithmetica*, **75-2** (1996), 105-117.

[9] C. Jordan, *Calculus of Finite Differences,* Chelsea Publ. Co., New York, 1950.

[10] M. Kaneko, Poly-Bernoulli numbers, *J. de Théorie des Nombres de Bordeaux*, **9** (1997), 221-228.

[11] T. Q. T. Le and J. Murakami, Kontsevich's integral for the Homfly polynomial and relations between values of multiple zeta functions, *Topology and its Applications*, **62** (1995), 193-206.

[12] L. Lewin, *Polylogarithms and Associated Functions*, Tata Institute, Bombey, 1980.

[13] Y. Ohno, A generalization of the duality and sum formulas on the multiple zeta values, *preprint* (1997).

[14] 大野泰生, 多重ゼータ値の関係式について, 第5回整数論サマースクール報告集 (1997), 197-204.

[15] 大野泰生, 多重ゼータ値の関係式と、多重ベルヌーイ数に関連するゼータ関数について, 津田塾大学数学・計算機科学研究所報, 15, 第3回津田塾大学整数論シンポジウム報告集 (1998), 98-107.

[16] C. L. Siegel, *Advanced Analytic Number Theory*, Chelsea Publ. Co., New York, 1950.

[17] L. Tornheim, Harmonic double series, *Amer. J. Math.*, 72 (1950), 303-314.

[18] D. Zagier, Values of zeta functions and their applications, in ECM volume, *Progress in Math.*, 120 (1994), 497-512.

Yasuo Ohno

Department of Mathematics
Graduate school of Science
Osaka University
Machikaneyama 1-1
Toyonaka, Osaka, 560-0043 Japan
e-mail: ohno@math.sci.osaka-u.ac.jp

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straβe 26
53225 Bonn, Germany
('98.12.31. まで)

符号と Siegel modular form について

対島 浩司 (筑波大 数学研究科)

ここでは. Coding theory と Siegel modular form に関連した. B. Runge 氏の予想 [7] について述べます.

この内容は. 小木曽岳義氏(筑波大数学系)との共同研究で得られたものです. 詳細は. [7] において発表される予定です.

1. 準備.

以下. 特に断わらない限り. n, g は正の整数とする.

1-1 code

- $\mathbb{F}_2^n = (\mathbb{Z}/2\mathbb{Z})^n$ の線型部分空間 C を code C という. このとき. n を code C の長さという.

  $C \ni {}^\forall c = (c_1, \cdots, c_n)$ に対して. c の重さ $wt(c)$ とは. $wt(c) := \#\{j \mid c_j \neq 0\}$.

  $\mathbb{F}_2^n \ni x = (x_1, \cdots, x_n)$, $y = (y_1, \cdots, y_n)$ に対して. x と y の内積 $\langle x, y \rangle$ とは.

  $$\langle x, y \rangle := x_1 y_1 + \cdots + x_n y_n .$$

  code C の dual code $C^\perp$ とは. $C^\perp := \{x \in \mathbb{F}_2^n \mid \langle x, y \rangle = 0 \text{ for } {}^\forall y \in C\}$.

- code C が self-dual $\overset{\text{def}}{\Leftrightarrow}$ $C = C^\perp$.

  code C が doubly-even $\overset{\text{def}}{\Leftrightarrow}$ ${}^\forall c \in C$ の重さが 4 で割れる.

1-2 Siegel modular form

- Siegel 上半空間 $\mathbb{H}_g := \{ Z = X + iY \in M(g, \mathbb{C}) \mid {}^tZ = Z,\ Y > 0 \}$.
- Siegel modular 群 $\Gamma_g := Sp(g, \mathbb{Z})$.
  なお. $Sp(g, \mathbb{R}) \ni X = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ は. $\mathbb{H}_g \ni Z$ に対して. $X\langle Z \rangle := (AZ+B)(CZ+D)^{-1}$ により. 推移的に作用する.
- Siegel modular 形式 : 以下では. $g \geq 2$ とする.
  $k \in \mathbb{Z}_{\geq 0}$ に対して. $\mathbb{H}_g$ 上の正則関数 $f(Z)$ が. Γ_g に対する重さ k の (Siegel) modular 形式 とは. $\forall X = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_g$ に対して. $f(X\langle Z \rangle) = \det(CZ+D)^k f(Z)$ を満たすときをいう.
- $[\Gamma_g, k]$ で 同じ重さ k について (Γ_g に対する) modular 形式 全体のなす空間を表す
  $\bigoplus_k [\Gamma_g, k]$ で. $[\Gamma_g, k]$ の重さ k に関する直和を表す
  なお. $[\Gamma_g, k]$ はベクトル空間になり. $\bigoplus_k [\Gamma_g, k]$ は有限生成 graded ring になる.

1-3 Theta 関数

- Theta 関数 $\theta\begin{bmatrix} \alpha \\ \beta \end{bmatrix}(\tau, z) := \sum_{x \in \mathbb{Z}^g} \exp\left(2\pi i \left(\frac{1}{2} t[x + \frac{1}{2}\alpha]\tau + \langle x + \frac{1}{2}\alpha,\ z + \frac{1}{2}\beta \rangle \right) \right)$.
  但し. $\tau \in \mathbb{H}_g,\ z \in \mathbb{C}^g$ であり.
  $t[x] := {}^t x \tau x$. $\langle , \rangle$: 普通の内積. $\alpha, \beta \in \mathbb{F}_2^g$ である.
- $\theta\begin{bmatrix} \alpha \\ \beta \end{bmatrix}(\tau, 0)$ を Theta constant という.
- $f_\alpha := \theta\begin{bmatrix} \alpha \\ 0 \end{bmatrix}(2\tau, 0)$ を Thetas of second order という.

2. 予想とその背景

B. Runge は、[8] において、次の Th. A を証明しました

Th. A (Runge)

$\forall a=(a_1,\cdots,a_g)\in \mathbb{F}_2^g$ について、関数 $\gamma_a : \mathbb{F}_2^{2g}\times\cdots\times\mathbb{F}_2^{2g} \longrightarrow \mathbb{Z}_+$ を

$\gamma_a(\eta_1,\cdots,\eta_g) := \#\left\{ i \mid a'\eta_{i,1},\cdots,\eta_{i,g}) \right\}$, $(\eta_1,\cdots,\eta_g) = \begin{pmatrix} \eta_{11}\cdots\eta_{1g} \\ \vdots \\ \eta_{2n}\cdots\eta_{2g} \end{pmatrix}$

と定義する.

このとき、self-dual で doubly-even な $\mathbb{F}_2^{2n}$ の code C に対する多項式

$$P_g(C) := \sum_{(\eta_1,\cdots,\eta_g)\in C^g} \prod_{a\in\mathbb{F}_2^g} f_a^{\gamma_a(\eta_1,\cdots,\eta_g)}$$

において、f_a を Thetas of second order $f_a = \vartheta\begin{bmatrix} a \\ 0 \end{bmatrix}(2\tau,0)$ とすると、

Γ_g に対する重さ $k=\frac{n}{2}$ の modular 形式になる.

この Th. A により、特に $g=2$ の場合は、多項式 $P_2(C)$ により生成される空間から、ある有限群 G による不変式環 $\mathbb{C}[f_a ; a\in\mathbb{F}_2^2]^G$ が得られることがわかっています ([1], [2] も併せて参照して下さい).

又、この Th. A は、Siegel modular 群 Γ_g についての主張ですが、井草準一先生の 1960年代の一連の研究結果 ([3]~[6]) から、$g=2$ の場合は、次に定義する Theta 群 $\Gamma_2(1,2)$ についても主張は正しいことがわかります.

Theta 群 $\Gamma_2(1,2) := \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix}\in\Gamma_2 \;\middle|\; (A^tB)_0 \equiv (D^tC)_0 \equiv 0 \mod 2 \right\} \subset \Gamma_2$.

但し、$(M)_0$ は、M の対角成分からなる縦ベクトルを表す.

そして. Rungeは. Theta群 $\Gamma_2(1,2)$ に対応する有限群 G として.

$$G = \left\langle S_4,\ \begin{pmatrix} \pm 1 & \\ & \pm 1_{\pm 1} \end{pmatrix},\ \frac{1+i}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \right\rangle \subset GL(4,\mathbb{C})$$

を採用し. 更に[10]に於いて. 次のTh. Bを証明しました.

(有限群 G の構成に関しては. [9]. [10]を参照して下さい)

Th. B (Runge)

$$\bigoplus_{2|k} [\Gamma_2(1,2), k] = \mathbb{C}[P_2^4, P_2^3P_6, P_2^2P_6^2, P_2P_6^3, P_6^4, P_8, P_{12}]$$

但し. P_i は i 次の斉次多項式である.

次いで. [10]に於いて. このTh. Bの任意の重さへの拡張として. Rungeは次の予想もしました.

予想 (Runge)

$\bigoplus_k [\Gamma_2(1,2), k]$ は次のような構造をもつだろう:

$$\bigoplus_k [\Gamma_2(1,2), k] = \mathbb{C}[P_2^4, P_2^3P_6, P_2^2P_6^2, P_2P_6^3, P_6^4, P_8, P_{12}, P_{28}\Theta, P_{32}\Theta, P_{36}\Theta].$$

但し. P_i は i 次の斉次多項式.

$$\Theta := \prod_{even} \theta\begin{bmatrix} x \\ \beta \end{bmatrix}(\tau, 0).$$

予想に於いて. Θ は10次であることに注意します.

又. [8]. [10]では. P_2. P_6. P_8 及び P_{12} の具体的な形が計算されています.

従って. 特に. P_{28}. P_{32} 及び P_{36} の具体的な形を計算する必要があります.

3. 主要結果

我々は、P_{28}, P_{32} 及び P_{36} が、上の有限群 G の作用によって不変であることを確かめ、次の具体的な形を決定しました：

$$P_{28} = (19,5,3,1)^A - 3(17,7,3,1)^A + (15,9,3,1)^A - 6(15,7,5,1)^A + 5(13,11,3,1)^A + 16(13,9,5,1)^A - 54(13,7,5,3)^A + 13(11,9,7,1)^A - 39(11,9,5,3)^A .$$

$$P_{32} = (21,7,3,1)^A - 7(19,9,3,1)^A + 21(17,11,3,1)^A - 63(17,7,5,3)^A - 35(15,13,3,1)^A - 18(15,9,7,1)^A + 203(15,9,5,3)^A + 63(13,11,7,1)^A - 294(13,11,5,3)^A - 322(13,9,7,3)^A + 2457(11,9,7,5)^A .$$

$$P_{36} = 15(25,7,3,1)^A - 25(23,9,3,1)^A + 46(23,7,5,1)^A + 120(21,11,3,1)^A - 276(21,9,5,1)^A - 1074(21,7,5,3)^A + 644(19,13,3,1)^A - 135(19,9,7,1)^A + 1610(19,9,5,3)^A - 210(17,15,3,1)^A - 644(17,13,5,1)^A + 266(17,11,5,3)^A - 1665(17,9,7,3)^A + 1254(15,13,7,1)^A - 1330(15,13,5,3)^A + 1956(15,11,9,1)^A - 8736(15,11,7,3)^A + 34690(15,9,7,5)^A - 15750(13,11,9,3)^A + 20930(13,11,7,5)^A .$$

但し、$(a_1,a_2,a_3,a_4)^A := \sum_{\sigma\in S_4} \mathrm{sign}(\sigma) \prod_{i=1,\dots,4} (t_{i-1}^{a_3})^\sigma$ としています.

更に、この計算結果を用いて、$Q_{48} := P_2^3 P_6 P_{36}$ と定義し、このQ_{48}が
$P_2^4 P_{12} P_{28}$, $P_8 P_{12} P_{28}$, $P_8 P_2^4 P_{32}$, $P_8^2 P_{32}$, $P_{12}^2 P_{32}$, $P_{12} P_{36}$
たちの線型結合で表わせないことも確かめ、予想の環が次の分解をもつ
ことを示しました:

$$\begin{aligned}
\bigoplus_{\ell} [\Gamma_2(1,2),\ell] &= \mathbb{C}[P_2^4, P_2^3P_6, P_2^2P_6^2, P_2P_6^3, P_6^4, P_8, P_{12}, P_{28}\textcircled{1}, P_{32}\textcircled{1}, P_{36}\textcircled{1}] \\
&= \mathbb{C}[P_2^4, P_6^4, P_8, P_{12}] \\
&\quad \oplus \mathbb{C}[P_2^4, P_6^4, P_8, P_{12}]\, P_2^3P_6 \\
&\quad \oplus \mathbb{C}[P_2^4, P_6^4, P_8, P_{12}]\, P_2^2P_6^2 \\
&\quad \oplus \mathbb{C}[P_2^4, P_6^4, P_8, P_{12}]\, P_2P_6^3 \\
&\quad \oplus \mathbb{C}[P_2^4, P_6^4, P_8, P_{12}]\, P_{28}\textcircled{1} \\
&\quad \oplus \mathbb{C}[P_2^4, P_6^4, P_8, P_{12}]\, P_{32}\textcircled{1} \\
&\quad \oplus \mathbb{C}[P_2^4, P_6^4, P_8, P_{12}]\, P_{36}\textcircled{1} \\
&\quad \oplus \mathbb{C}[P_2^4, P_6^4, P_8, P_{12}]\, P_2^3P_6P_{36}\textcircled{1}.
\end{aligned}$$

このようにして、予想も証明することができました.

4. 参考文献

[1] 坂内英一，有限群の不変式環と保型形式（A Survey），第41回代数学シンポジウム報告集（1996），173－187．

[2] ———，代数的組合せ論の視点，岩波講座 現代数学の広がり2（1997），129－172．

[3] J. Igusa, On Siegel modular forms of genus two, Amer. J. Math., 84 (1962), 175－200.

[4] ———, On Siegel modular forms of genus two (II), Amer. J. Math., 86 (1964), 392－412.

[5] ———, On the graded ring of theta constants, Amer. J. Math., 86 (1964), 219－246.

[6] ———, On the graded ring of theta constants (II), Amer. J. Math., 88 (1966), 221－236.

[7] T. Kojiso & K. Tsushima, On an algebra of Siegel modular forms associated with the theta group $\Gamma_2(1,2)$, to appear in Tsukuba J. Math.

[8] B. Runge, On Siegel modular forms Part I, J. reine. angew. Math., 436 (1993), 57－85.

[9] ———. On Siegel modular forms Part II. Nagoya Math. J. 138 (1995). 179-197.

[10] ———. Codes and Siegel modular forms. Disc. Math.. 148 (1996). 175-204.

対称群のねじれ群環と Lie superalgebra の duality

山口 学

1. 概要.

k 対称群の有限次元既約表現の指標公式 (Frobenius の公式) [Fr] (cf. [Ma])

$$p_\mu(x) = \sum_{\lambda \in P_k} \chi_\lambda(\mu) s_\lambda(x) \qquad (\mu \in P_k)$$

は、対称群と一般線型群の表現の相対関係 (Schur-Weyl の相対関係) をあらわしている。ここに、P_k は k の分割 (partition) 全体、$p_\mu(x)$ はべき和対称関数、$s_\lambda(x)$ は Schur 関数、$\chi_\lambda(\mu)$ は λ に対する k 次対称群の既約指標χ_λ が型 (cycle type) μ の共役類の元で取る値をあらわす。

この研究では、k 対称群の有限次元既約射影表現の指標公式 [Sc] (cf. [Stl])

$$(\sqrt{2})^{l(\mu)} p_\mu(x) = \sum_{\lambda \in DP_k} \varphi_\lambda(\gamma^\mu)(\sqrt{2})^{-l(\lambda)-\varepsilon(\lambda)} Q_\lambda(x) \qquad (\mu \in OP_k)$$

に、表現論的意味付けを与えた。すなわち、対称群のねじれ群環と queer Lie superalgebra との表現の相対関係を示した。ただし、上の指標公式において、

$$DP_k = \{\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_l) \in P_k \mid \lambda_1 > \lambda_2 > \cdots > \lambda_l\}$$
$$OP_k = \{\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_l) \in P_k \mid \lambda_i : \text{odd} \ \ (1 \le i \le l)\}$$

であり (DP_k の元は distinct partition と呼ばれる)、Q_λ は Schur の Q-関数と呼ばれる対称関数である (cf. [Ma])。

2. ねじれ群環 $\mathcal{A}_k$, $\mathcal{B}_k$ と Clifford 代数 $\mathcal{C}_k$.

Definition 1. (対称群のねじれ群環 $\mathcal{A}_k$)

$k \ge 1$ を自然数とする。$\mathcal{A}_k$ を、次の生成元と関係式で定義される $\mathbb{C}$ 上の代数とする。

生成元： $\gamma_1, \ldots, \gamma_{k-1}$

関係式： $\gamma_i^2 = -1 \ \ (1 \le i \le k-1)$, $(\gamma_i \gamma_{i+1})^3 = -1 \ \ (1 \le i \le k-2)$,
$(\gamma_i \gamma_j)^2 = -1 \ \ (|i-j| \ge 2)$

$\mathcal{A}_k$ は k 次対称群のねじれ群環である。k 次対称群のねじれ群環は同型をのぞけば、通常の群環と $\mathcal{A}_k$ の 2 つだけである (cf. [St1])。一般に、有限群の $\mathbb{C}$ 上のねじれ群環は半単純 (いくつかの完全行列環の直和に同型) である。

ここでは、$\deg \gamma_i = 1 \in \mathbb{Z}/2\mathbb{Z} = \{0,1\}$ $(1 \leq i \leq k-1)$ として、$\mathcal{A}_k$ を $\mathbb{Z}/2\mathbb{Z}$-次数つき環と見なす。

$\mathbb{Z}/2\mathbb{Z}$-次数つき環 $A = A_0 \oplus A_1$ の表現といったら、$\mathbb{Z}/2\mathbb{Z}$-次数つきのものだけを考える。つまり、2 つのベクトル空間への直和分解をもつ $V = V_0 \oplus V_1$ と写像 $\rho\colon A \to \mathrm{End}(V)$ の組 (ρ, V) が、A の表現であるとは、ρ が次数つき環の準同型であることと、すなわち、$\rho(A_\alpha)V_\beta \subset V_{\alpha+\beta}$ $(\alpha, \beta \in \mathbb{Z}/2\mathbb{Z})$ が成立することである。混同する恐れのないときは、$\rho(a)v = av$ $(a \in A, v \in V)$ とかく。このとき、A-加群 V の中心化環 $\mathrm{End}^{\cdot}_A(V)$ を次で定義する。

$$\mathrm{End}^{\alpha}_A(V) = \left\{ f \in \mathrm{End}(V) \mid \begin{array}{l} f(V_\beta) \subset V_{\alpha+\beta} \ (\beta \in \mathbb{Z}/2\mathbb{Z}) \\ f \circ \rho(a) = (-1)^{\alpha\cdot\gamma} \rho(a) \circ f \ (a \in A_\gamma) \end{array} \right\} \quad (\alpha \in \mathbb{Z}/2\mathbb{Z})$$

$$\mathrm{End}^{\cdot}_A(V) = \mathrm{End}^{0}_A(V) \oplus \mathrm{End}^{1}_A(V)$$

Definition 2. (B_k 型 Weyl 群のねじれ群環 $\mathcal{B}_k$)

$\mathcal{B}_k$ を、次の生成元と関係式で定義される $\mathbb{C}$ 上の代数とする。

生成元： $\tau, \sigma_1, \ldots, \sigma_{k-1}$

関係式： $\tau^2 = \sigma_i^2 = 1 \quad (1 \leq i \leq k-1), \quad (\sigma_i\sigma_{i+1})^3 = 1 \quad (1 \leq i \leq k-2),$
$(\sigma_i\sigma_j)^2 = 1 \quad (|i-j| \geq 2), \quad (\tau\sigma_i)^2 = 1 \quad (2 \leq i \leq k-1),$
$(\tau\sigma_1)^4 = -1$

$\mathcal{B}_k$ は B_k 型 Weyl 群 $W(B_k)$ のねじれ群環の一つである。$W(B_k)$ のねじれ群環の同型類は、8 個ある (cf. [DM], [St2])。$\deg \tau = 1$, $\deg \sigma_i = 0$ $(1 \leq i \leq k-1)$ として、$\mathcal{B}_k$ を $\mathbb{Z}/2\mathbb{Z}$-次数つき環と見なす。

Definition 3. (Clifford 代数 $\mathcal{C}_k$)

$\mathcal{C}_k$ を、次の生成元と関係式で定義される $\mathbb{C}$ 上の代数とする。

生成元： $\xi_1, \ldots, \xi_k$

関係式： $\xi_i^2 = 1$ $(1 \leq i \leq k)$, $\quad \xi_i\xi_j = -\xi_j\xi_i$ $(i \neq j)$

$\mathcal{C}_k$ は $(\mathbb{Z}/2\mathbb{Z})^{\times k}$ のねじれ群環である。$\deg \xi_i = 1$ $(1 \leq i \leq k)$ として、$\mathcal{C}_k$ を $\mathbb{Z}/2\mathbb{Z}$-次数つき環と見なす。

$\mathbb{Z}/2\mathbb{Z}$-次数つき環 A, B のテンソル積を考える。テンソル積空間 $A \otimes B$ 上に、積を $(a \otimes b)(c \otimes d) = (-1)^{\alpha\cdot\beta} ac \otimes bd$ $(a \in A, b \in B_\alpha, c \in A_\beta, d \in B)$ で定義する。このテンソル積を、$A \dot{\otimes} B$ とあらわす。

Theorem 4. 次で定義される写像 $\vartheta\colon C_k \dot{\otimes} \mathcal{A}_k \to \mathcal{B}_k$

$$\vartheta(\xi_1 \dot{\otimes} 1) \mapsto \tau_i \quad (1 \le i \le k),$$
$$\vartheta(1 \dot{\otimes} \gamma_j) \mapsto \frac{1}{\sqrt{2}}(\tau_j - \tau_{j+1})\sigma_j \quad (1 \le j \le k-1)$$

は、$\mathbb{Z}/2\mathbb{Z}$-次数つき環の同型を与える。ここで、$\tau_i = \sigma_{i-1}\cdots\sigma_1\tau\sigma_1\ldots\sigma_{i-1}$ $(1 \le i \le k)$

通常の半単純環の表現のときは、上のような同型があるとき、$\mathcal{B}_k$ の既約表現は C_k と $\mathcal{A}_k$ の既約表現のテンソル積で得られるが、$\mathbb{Z}/2\mathbb{Z}$-次数つき環のときは、少し事情が異なる。既約表現の中心化環は 1 次元とは限らず、次の定理のようになる。

Theorem 5. rm(cf. [J]) ($\mathbb{Z}/2\mathbb{Z}$-次数つき環に対する Schur の補題)
A を $\mathbb{Z}/2\mathbb{Z}$-次数つき環、V を既約 A-加群とする。このとき、次のどちらかが成立する。
case 1. (type M と呼ぶ)

$$\mathrm{End}_{\dot{A}}(V) = \mathbb{C}\begin{pmatrix} I_m & 0 \\ 0 & I_n \end{pmatrix}$$
(ここで、$m = \dim V_0$, $n = \dim V_1$)

case 2. (type Q と呼ぶ)

$$\mathrm{End}_{\dot{A}}(V) = \mathbb{C}\begin{pmatrix} I_n & 0 \\ 0 & I_n \end{pmatrix} \oplus \mathbb{C}\begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}$$
(このときは、$\dim V_0 = \dim V_1 = n$ となる)

V, W をそれぞれ A, B-加群とするとき、テンソル空間 $V \otimes W$ 上の $A \dot{\otimes} B$ の表現を $(a \dot{\otimes} b)(v \otimes w) = (-1)^{\alpha\cdot\beta} av \otimes bw$ $(a \in A, b \in B_\alpha, v \in V_\beta, w \in W)$ で定義する。このとき、既約加群のテンソル積は必ずしも既約になるわけではなく、詳しくは次のようになる。

Theorem 6. V, W をそれぞれ A, B-加群とする。
case 1. V も W も type M のとき、$V \otimes W$ は type M の既約 $A \dot{\otimes} B$-加群となる。
case 2. V もしくは W のいずれか一方が type M で、もう一方が type Q とき、$V \otimes W$ は type Q の既約 $A \dot{\otimes} B$-加群となる。
case 3. V も W も type Q のとき、$V \otimes W$ は 2 つの同型な type Q の既約部分 $A \dot{\otimes} B$-加群の直和と同型となる。
また、$A \dot{\otimes} B$ の既約加群はすべて上の形で得られ、とくに、

{既約 A-加群の同型類} × {既約 A-加群の同型類} $\tilde{\to}$ {既約 $A \dot{\otimes} B$-加群の同型類}

の 1 対 1 対応が得られる。

$\mathcal{B}_k$ の既約表現の話に戻る。上の Theorem 6 により、$\mathcal{B}_k$ の既約表現は Clifford 代数 C_k と対称群のねじれ群環 $\mathcal{A}_k$ を用いてあらわされる。実は、Clifford 代数 C_k は $\mathbb{Z}/2\mathbb{Z}$-次数つき環として単純 (0 と自分自身以外の $\mathbb{Z}/2\mathbb{Z}$-次数つき両側イデアルを持たない) であるので、既約加群は同型をのぞいて一意に定まる。それを X_k とおく。また、$\mathcal{A}_k$ の既約加群は DP_k で特徴づけられることが知られているので、それらを V_λ $(\lambda \in DP_k)$ とおく。

これらの既約加群が、いつ type M または type Q になるかは、次の条件による:

$$X_k = \begin{cases} \text{type } M & \text{if } k : \text{even} \\ \text{type } Q & \text{if } k : \text{odd} \end{cases}$$

$$V_\lambda = \begin{cases} \text{type } M & \text{if } k - l(\lambda) : \text{even} \\ \text{type } Q & \text{if } k - l(\lambda) : \text{odd} \end{cases}$$

$X_k \otimes V_\lambda$ の部分加群として得られる既約 $\mathcal{B}_k$-加群を W_λ とおくと、Theorem 6 より

$$W_\lambda = \begin{cases} \text{type } M & \text{if } l(\lambda) : \text{even} \\ \text{type } Q & \text{if } l(\lambda) : \text{odd} \end{cases}$$

となる。

Sergeev の相対関係.

Definition 7. (queer Lie superalgebra)

$\mathfrak{q}(n)$ は次で定義される Lie superalgebra (cf. [K]) である (queer Lie superalgebra と呼ばれる)。

$$\mathfrak{q}(n) = \left\{ \begin{pmatrix} E & F \\ F & E \end{pmatrix} \in M_{2n}(\mathbb{C}) \mid E, F \in M_n(\mathbb{C}) \right\}$$

$$\mathfrak{q}_0(n) = \left\{ \begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix} \right\}, \ \mathfrak{q}_1(n) = \left\{ \begin{pmatrix} 0 & F \\ F & 0 \end{pmatrix} \right\}$$

$$[\ ,\ ] : \mathfrak{q}(n) \times \mathfrak{q}(n) \to \mathfrak{q}(n) \quad \text{(Jacobi product)}$$

$$[X, Y] = XY - (-1)^{\alpha\cdot\beta} YX \quad (X, Y \in \mathfrak{q}(n))$$

$\mathcal{U}_n = \mathcal{U}(\mathfrak{q}(n))$ を $\mathfrak{q}(n)$ の包絡環とする。

$\mathfrak{q}(n)$ は (したがって $\mathcal{U}_n$ も) $\mathbb{C}$ 上 $2n$ 次元の $\mathbb{Z}/2\mathbb{Z}$-次数つきのベクトル空間 $V = \mathbb{C}^n \oplus \mathbb{C}^n$ に自然に作用する。余積 (coproduct) $\Delta : \mathcal{U}_n \to \mathcal{U}_n \dot{\otimes} \mathcal{U}_n$; $X \mapsto X \dot{\otimes} 1 + 1 \dot{\otimes} X$ を用いて、V の k 階テンソル積空間 $W = V^{\dot{\otimes} k}$ の上の $\mathcal{U}_n$ の表現 $\Theta : \mathcal{U}_n \to \mathrm{End}(W)$ が定義される。

$$\Theta(X)(v_1 \dot{\otimes} \cdots \dot{\otimes} v_k) = \sum_{j=1}^{k} (-1)^{\alpha\cdot(\beta_1 + \cdots + \beta_{j-1})} v_1 \dot{\otimes} \cdots \dot{\otimes} \overset{j}{\check{X}} v_j \dot{\otimes} \cdots \dot{\otimes} v_k$$

$$(X \in \mathfrak{q}(n)_\alpha,\ v_i \in V_{\beta_i}\ (1 \le i \le k),\ \alpha, \beta_i \in \mathbb{Z}/2\mathbb{Z}\ (1 \le i \le k))$$

そして、同じ空間 W 上の $\mathcal{B}_k$ の表現 $\Psi\colon \mathcal{B}_k \to \mathrm{End}(W)$ が次のように定義される (cf. [Se])。

$$\Psi(\tau)(v_1 \dot{\otimes} \cdots \dot{\otimes} v_k) = (Pv_1) \dot{\otimes} v_2 \dot{\otimes} \cdots \dot{\otimes} v_k$$

$$\Psi(\sigma_i)(v_1 \dot{\otimes} \cdots \dot{\otimes} v_k) = (-1)^{\beta_i \cdot \beta_{i+1}} v_1 \dot{\otimes} \cdots \dot{\otimes} v_{i+1} \dot{\otimes} v_i \dot{\otimes} \cdots \dot{\otimes} v_k$$

$$(v_i \in V_{\beta_i},\ \beta_i \in \mathbb{Z}/2\mathbb{Z}.\ (1 \le i \le k-1))$$

$$P = \begin{pmatrix} 0 & -\sqrt{-1}I_n \\ \sqrt{-1}I_n & 0 \end{pmatrix} \in \mathrm{End}(V)$$

Theorem 8. [Se] (1) $\mathcal{B}_k$ と $\mathcal{U}_n$ は W 上にお互いに中心化環として作用する。つまり、次が成立する。

$$\mathrm{End}_{\Theta(\mathcal{U}_n)}(W) = \Psi(\mathcal{B}_k). \quad \mathrm{End}_{\Psi(\mathcal{B}_k)}(W) = \Theta(\mathcal{U}_n)$$

(2) $W_\lambda \subset W$ $(\nu \in DP_k) \iff l(\lambda) \le n$.

(1) が成立するとき、通常の半単純環のときと同じように (*$\mathbb{Z}/2\mathbb{Z}$-次数つき環の double centralizer theorem (cf. [Ya])* なるものが成立して) W の部分加群として現れる既約 $\mathcal{B}_k$-加群と既約 $\mathcal{U}_n$ 加群の間に 1 対 1 対応があることがわかり、次の既約表現のテンソル積への分解を得る。

$$W = \bigoplus_{\substack{\lambda \in DP_k \\ l(\lambda):\ \mathrm{even} \le n}} W_\lambda \otimes U_\lambda \ominus \bigoplus_{\substack{\lambda \in DP_k \\ l(\lambda):\ \mathrm{odd} \le n}} (W_\lambda \otimes U_\lambda)^\circ$$

ここで、U_λ $(\lambda \in DP_k)$ は W_λ に対応する既約 $\mathcal{U}_n$-加群であり、$\mathcal{B}_k$-加群 W_λ が *type M (resp. type Q)* であれば、対応する $\mathcal{U}_n$-加群 U_λ も *type M (resp. type Q)* となる。$^\circ$ は、*type Q* どうしの既約加群のテンソル積が同型な 2 つの既約加群に分解するときの既約加群の一つをあらわす。

(3) $\mathrm{Ch}[U_\lambda]$ を U_λ の指標 ((注) 参照) とする。

$$\mathrm{Ch}[U_\lambda](\mathrm{diag}(x_1, \ldots, x_n, x_1, \ldots . x_n)) = (\sqrt{2})^{d(\lambda)-l(\lambda)} Q_\lambda(x_1, x_2, \ldots . x_n)$$

(注) $\mathfrak{q}(n)_0 \cong \mathfrak{gl}(n, \mathbb{C})$ *(Lie* 環としての同型*)* を用いて、U_λ を $\mathfrak{gl}(n.\mathbb{C})$ の *(*したがって, $GL(n, \mathbb{C})$ の*)* 多項式表現と見なしたときの指標。

$\mathcal{A}_k$ と $\mathfrak{q}(n)$ の相対関係.

Thoerem 4 より $C_k \dot{\otimes} \mathcal{A}_k \cong \mathcal{B}_k$ である。C_k に属する互いに可換な $r = \lfloor k/2 \rfloor$ 個の元 $\zeta_j = \sqrt{-1}\xi_{2j-1}\xi_{2j}$ $(1 \le j \le r)$ を考える $(\zeta_j^2 = 1\ (1 \le j \le r)$ となる)。W を $\{\zeta_j\}_{1 \le j \le r}$ に関する同時固有空間に分解する:

$$W = \bigoplus_{\varepsilon = (\varepsilon_1, \ldots \varepsilon_r) \in \{0,1\}^r} W^\varepsilon$$

$$W^\varepsilon = \{w \in W \mid \zeta_j w = (-1)^{\varepsilon_j} w\}$$

次の定理を得る。

Theorem 9. 任意の $\varepsilon \in \mathbb{Z}_2^r$ に対して次が成立する。

(1) k 偶数のとき

$$W^\varepsilon \cong_{\mathcal{A}_k \dot{\otimes} \mathcal{U}_n} \bigoplus_{\substack{\lambda \in DP_k \\ l(\lambda):\text{even}}} V_\lambda \dot{\otimes} U_\lambda \ominus \bigoplus_{\substack{\lambda \in DP_k \\ l(\lambda):\text{odd}}} (V_\lambda \dot{\otimes} U_\lambda)^\circ$$

ここで、$\mathcal{A}_k$-加群 V_λ が *type M (resp. type Q)* であれば、対応する $\mathcal{U}_n$-加群 U_λ も *type M (resp. type Q)* となる。

さらに、$\mathcal{A}_k$ と $\mathcal{U}_k$ は W^ε 上に互いの中心化環として作用する。つまり、

$$\mathrm{End}^{\cdot}_{\Theta(\mathcal{U}_n)}(W^\varepsilon) = \Psi(\mathcal{A}_k), \quad \mathrm{End}^{\cdot}_{\Psi(\mathcal{A}_k)}(W^\varepsilon) = \Theta(\mathcal{U}_n)$$

(2) k が奇数のとき

$$W^\varepsilon \cong_{\mathcal{A}_k \dot{\otimes} \mathcal{U}_n} \bigoplus_{\lambda \in DP_k} V_\lambda \dot{\otimes} U_\lambda$$

ここで、$\mathcal{A}_k$-加群 V_λ が *type M (resp. type Q)* であれば、対応する $\mathcal{U}_n$-加群 U_λ も *type Q (resp. type M)* となる。

さらに、互いの中心化環は、*Cliffford* 代数とのテンソル積である。

$$\mathrm{End}^{\cdot}_{\Theta(\mathcal{U}_n)}(W^\varepsilon) \cong \mathcal{C}_1 \otimes \Psi(\mathcal{A}_k). \quad \mathrm{End}^{\cdot}_{\Psi(\mathcal{A}_k)}(W^\varepsilon) \cong \mathcal{C}_1 \otimes \Theta(\mathcal{U}_n)$$

References

[DM] J. W. Davies. A. O. Morris, *The Schur multiplier of the generalized symmetric group.* J. London Math. Soc. Ser. 2 **8** (1974), 615-620.

[Fr] F. G. Frobenius, *Über die Charaktere der symmetrischen Gruppe.* Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin (1900), 516-534.

[Jo] T. Józefiak, *Semisimple superalgebras.* in: Some Current Trends in Algebra. Proceedings of the Varna Conference 1986. Lecture Notes in Math. 1352. Springer Berlin (1988). 96-113.

[Ka] V. G. Kac, *Lie superalgebras*, Adv. in Math. **26** (1977). 8-96.

[Ma] I. G. Macdonald, *Symmetric functions and Hall polynomials.* Clarendon Press, Oxford (1979).

[Sc] I. Schur, *Über die Darrstellung der symmetrischen und der alternierenhen Gruppe durch gebrohene lineare Substitutionen*, J. Reine Angew. Math. **139** (1911). 155-250.

[Se] A. N. Sergeev, *Tensor algebra of the identity representation as a module over Lie superalgebras $GL(n, m)$ and $Q(n)$*, Math. USSR Sbornik **51**, No. **2** (1985). 419-425.

[St1] J. R. Stembridge. *Shifted Tableaux and the Projective Representations of Symmetric groups.* Adv. in Math. **74** (1989), 87-134.

[St2] J. R. Stembridge. *The Projective Representations of the Hyperoctahedral Group.* J. Algebra **145** (1992), 396-453.

[Ya] M. Yamaguchi, *A duality of the twisted group algebra of the symmetric grouyp and a Lie superalgebra*, to appear in J. Algeba.